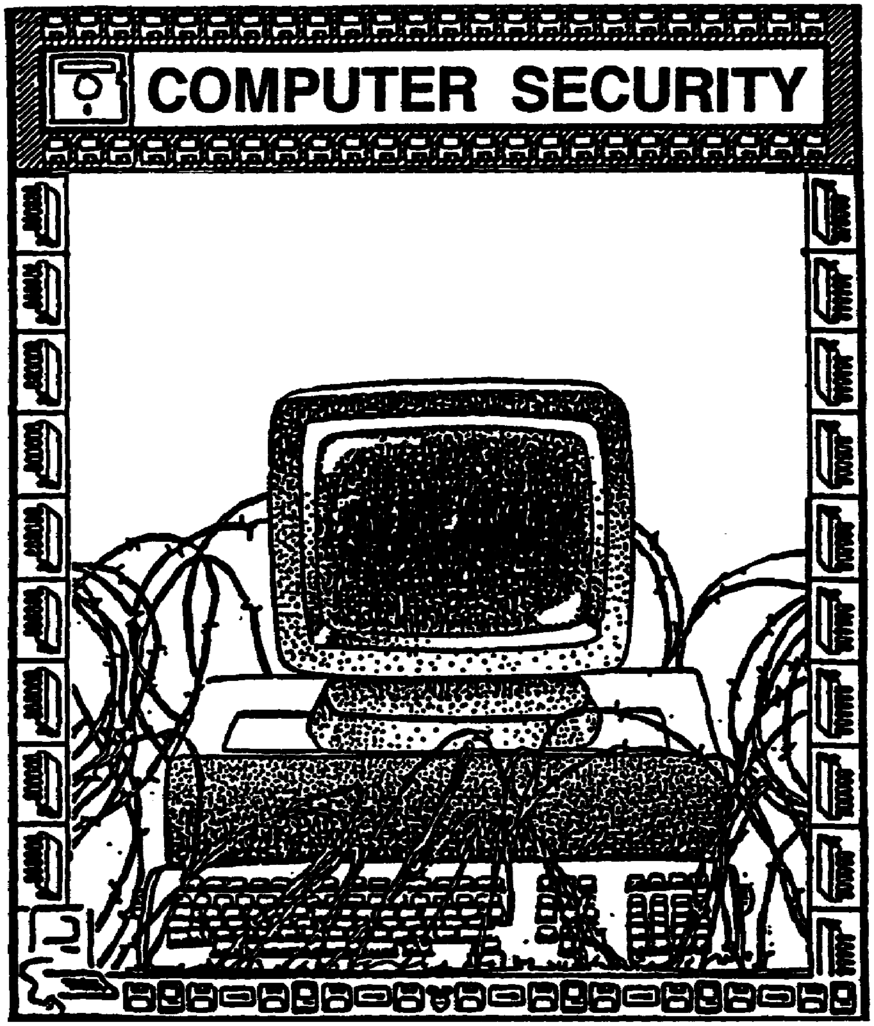
SUBCOURSE
IT0772

EDITION
D

US ARMY INTELLIGENCE CENTER



THE ARMY INSTITUTE FOR PROFESSIONAL DEVELOPMENT

ARMY CORRESPONDENCE COURSE PROGRAM

A I P D

READINESS
PROFESSIONALISM
THRU
GROWTH

Computer Security

Subcourse Number IT0772

EDITION D

United States Army Intelligence Center
Fort Huachuca, Arizona 85613-600

7 Credit Hours

Edition Date: May 1998

SUBCOURSE OVERVIEW

This subcourse is designed to teach you the basic procedures for protecting computers and the information processed on them. Instructions are contained within this subcourse on the fundamental theory underlying computer security, the threats to computer, the accreditation process, and the implementation of computer security countermeasures.

There are no prerequisites for this subcourse.

This subcourse reflects the doctrine which was current at the time the subcourse was prepared. In your own work situation, always refer to the latest publications.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

TERMINAL LEARNING OBJECTIVES

ACTION: You will identify procedures for: protecting computer and the information processed, recognizing the threats to computers, determining sensitivity levels, accomplishing system accreditation, and selecting and applying computer security countermeasures.

CONDITIONS: You will be given narrative information and extracts from AR 380-19.

STANDARDS: You will protect Army computers and the information processed on them in accordance with AR 380-19 and related security publications.

TABLE OF CONTENTS

LESSON 1

COMPUTER SECURITY OVERVIEW

CRITICAL TASK: NONE.

OVERVIEW

LESSON DESCRIPTION:

In this lesson, you will learn the fundamental theory underlying computer security.

TERMINAL LEARNING OBJECTIVE:

ACTIONS:	Identify and define the four sub-disciplines (sub-securities) included in Information Systems Security, define sensitive defense information, and identify computer security responsibilities and appointments
CONDITIONS:	You will be given narrative information and extracts form AR 380-19.
STANDARDS:	You will be able to provide security advice and assistance for local units in accordance with the provisions of AR 380-19.
REFERENCES:	The material contained in this lesson was derived from the following publications:

AR 380-5
AR 380-19
AR 380-67
AR 381-20
DOD 5200.224M
FM 19-30
FM 101-5

INTRODUCTION

The Automated Systems Security Incident Support Team (ASSIST) of the Defense Information Systems Agency (DISA) tested the vulnerability of 12,000 DOD host computers in the unclassified domain. They found that 1-3% of the systems had exploitable front doors and that 88% could be penetrated by network trust relationships. Only 4% of the penetrations were detected and, of those, only 5% reported.

Why Systems are Vulnerable. There are many reasons why systems are vulnerable to attack:

Security is hard and expensive. It is not easy to design systems that resist penetration, particularly in today's world where they are connected to open networks. It requires considerable skill and investment of resources, often involving dozens of engineers and scientists and years of work. Consequently, many systems have vulnerabilities which allow an intruder to bypass the security controls. In many cases, the security controls themselves introduce weaknesses.

Security is a bottomless pit. It is often said that the only way to make a system secure is to pull the plug. It is not practical, and usually impossible, to achieve 100% security. Not only is it too expensive, it is unachievable because not all weaknesses and attacks can be anticipated. Vulnerabilities can be found in even carefully designed products. New methods of attack are continually being discovered. Thus, one settles for something less than perfect, say a 90% solution aimed at preventing the simplest and most common attacks. However, this brings me to the next observation:

Security is complex and fuzzy. We speak about information security as though it were well-defined and quantifiable. In fact, it is neither of these. Security policies are often complex, imprecise, sometimes conflicting, and subject to human judgment.

Organizations are willing to take risks. Organizations generally do not demand perfect security for their systems and information. They are willing to take risks, as they do with other assets and technologies, in order to save time and money, to enjoy the benefits of the Internet and new services, to boost productivity, and to ensure that their employees and customers are not denied legitimate access. Many organizations connect to the internet knowing fully well that they may be vulnerable to attack. Access to people, organizations, and information worldwide is considered well worth the risk. Security is about risk management, not absolute prevention.

Developers and users have limited resources. System developers have limited resources to spend on product development, and those resources have competing demands, including functionality, performance, and customer support. Decisions are based on factors such as marketability and profitability. Similarly, organizations have limited resources. Funds for security management, products, and training are balanced with other needs of the organization. In many organizations, the senior management do not view security as very important.

New technology is constantly emerging. New technologies, for example, to support World Wide Web applications, bring forth new forms of vulnerabilities. In the rush to bring products to market and increase connectivity, the security implications are not always thoroughly researched and understood. Weaknesses are not discovered until after the products have been on the market Security engineering lags behind the product development curve.

Security involves humans. Human beings are responsible for designing, configuring, and using systems with security features. They make mistakes in judgment and in implementation. They take shortcuts. They do not anticipate all possible failures. They can be conned by those wishing to intrude.

Hackers often justify their cracking activities with the argument that systems should be secure; they are merely exposing flaws that never should have appeared in the first place and should be fixed. This argument falls apart, however, in the context of the preceding analysis. Networked systems will always have vulnerabilities, just as our streets, homes, and other public infrastructures do. Breaking into a computer system, without authorization to do so, is no more ethical than breaking into a house to demonstrate its physical vulnerabilities.

Part A: What is computer security?

Computer security is about risk management, not absolute security, and involves application of both technical and non-technical countermeasures. Non-technical defenses include formulating a security policy for the organization and educating users about that policy.

Part B: How does computer security involve you?

As intelligence personnel, you will probably use computers to do your job. You will be responsible for the security of the computers you use, and for the security of the classified and sensitive information you process.

Your commander will expect you to be not only an intelligence expert, but also a security expert. if your commander has a security problem, to include a computer security problem, he will expect you to have the expertise to solve that problem.

The lessons in this subcourse are designed to provide you with the basic understanding of computer security that you will need as intelligence personnel. Most information in these lessons applies to the security of any computer, large or small. However, the primary intent is to provide security guidance on protecting the Army's personal computers (PCs) and the classified and unclassified-sensitive information they process.

Part C: Computer Security

Computer Security (COMPUSEC) is a sub-discipline (sub-security) of Information Systems Security (ISS). As well as using computers for familiar information processing functions, such as word processing, personnel management, and issuing your end-of-month paycheck, the Army uses computers and computer-based systems for a wide variety of other functions.

First, you use your PCs word processing program to type a message on a DD Form 173. Then the signal folks at the communications center use a computer-based communications system to transmit that message. Even the gunner on an M-1 tank deals with computers on a daily basis; the 60's main gun has a computer-based fire control system. This lesson will introduce you to ISS.

Part D: The U.S. Army Computer Security Program

The Army's Telecommunications and Automated Information Systems (TAIS) have certain inherent security vulnerabilities and these systems are known to be targeted by foreign intelligence services. ISS is defined as "a composite of means to protect telecommunications systems and automated information systems, and the information they process". ISS is a unified approach to protecting these systems, and the classified end unclassified-sensitive information processed by these systems.

A security “vulnerability” is a “weakness” in security. "Inherent” means that these security vulnerabilities are a fact of life. A basic principle of Physical Security is there is no such thing as an impenetrable barrier" and this principle applies to information processing as well; no matter how well we do in planning and applying security measures, there is no such thing as a completely secure computer!

AR 380-19, Information Systems Security, establishes the U.S. Army Information Systems Security Program (ISSP). The ISSP has been created in recognition of the Army’s widespread use of TAIS and the special problems involved with their security. The first step in understanding ISS is to understand some of the terms used in this lesson and in AR 380-19:

Telecommunications system: A “telecommunications system" is any system which transmits, receives, or otherwise communicates information by electrical, electromagnetic, electro-mechanical, or electro-optical means. A telecommunications system may include features normally associated with computers. You would find one of these systems in a “communications center.” Most state-of-the-art Army communications centers use telecommunications systems which are computer-based and look like a computer system.

Automated information system (AIS): An AIS is any assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information in electronic form, including stand-alone computers, small computers, word processors, multi-user computers, terminals, and networks. Included are the small computers, PCs, and word processing systems which will be found in the typical Army office. This equipment is often referred to as "office automation” systems.

Telecommunications and automated information system (TAIS): This term is used to refer to both telecommunications systems and automated information systems.

NOTE: To make it easy for you to follow the instruction, the term "computer" will be generally used throughout the lessons on “Computer Security," rather than the term “AIS.” “Computer” is a term you are familiar with and any policy that applies to an “AIS” naturally applies to a “computer".

Part E: Information Systems Security

ISS is an “umbrella” term which includes four sub-disciplines (or sub-securities):

Communications Security (COMSEC): COMSEC includes the measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and to ensure the authenticity of such telecommunications. Any time we communicate, unauthorized persons can intercept these communications. If we are using telephones, unauthorized persons can tap the wire and listen to our conversation. If we are using radios, unauthorized persons can use their radios to listen to what we are talking about. COMSEC includes things which protect these communications from intercept. One way of protecting our communications is by using encryption devices which turn plain English text into a meaningless jumble of letters.

Electronic Security (ELSEC): ELSEC includes the measures designed to deny unauthorized persons information of value derived from the interception and analysis of noncommunications electromagnetic radiations, such as radar. Each type of radar gives off unique signals and the enemy can use these signals to their advantage. For example, if a certain type of radar is only found in an artillery unit, any time the enemy detects that radar he knows there is an artillery unit in the area.

TEMPEST: TEMPEST, which is not an acronym, is the investigation, study, and control of compromising emanations from electrical or electronic equipment. Computers, electronic typewriters, and other such equipment send out signals when they are being used. If unauthorized persons have access to the right location and have the right equipment, they can intercept these signals and figure out what is being typed or processed by a computer or electronic typewriter.

Computer Security (COMPUSEC:): COMPUSEC includes all of the security measures and controls that protect computers, and the information processed, against unauthorized (accidental or intentional) disclosure, modification, or destruction.

Part F: Major Security Objectives

A good way to start our discussion of computer security is to take a look at what we are trying to achieve. Regardless of the type, model, or size of computer that we use to process classified information or unclassified-sensitive information, there are three major security objectives which must be met

Confidentiality: Classified defense information must, of course, be protected from unauthorized disclosure. However, certain unclassified-sensitive information, like For Official Use Only (FOUO) information, must also be protected. As well as protecting the Army's official information, you want to make sure that any computer which contains personal information about you is protected from unauthorized access. You don't want a stranger getting access to your medical records or your 201 file.

Integrity: Information must be protected against unauthorized changes and modification. Commanders use computer-based information to make important decisions and that information must be accurate. A decision based on incorrect information, will probably be the wrong decision. Imagine the impact on national security if some other county got Into US Army Personnel Central Clearance Facility (CCFs) computer and started granting security clearances. If you have ever had trouble getting a loan, you can appreciate the need for accuracy. One credit reporting agency did a survey of its records and found out that one third of the credit information they had on file was incorrect!

Availability: The Army depends on computers to perform its mission. Therefore, the Amy's computer systems, the information processed, and the services provided must be protected from deliberate or accidental loss, destruction, or interruption of services. We are totally dependent on computers and without them we probably can't do our jobs!

Part G: Sensitive Defense Information

The information which must be protected from unauthorized exploitation (unauthorized disclosure, modification, or destruction) includes both classified information and unclassified-sensitive information. The following are the types of information which the Army considers to be Sensitive Defense Information:

Classified information: In accordance with AR 380-5, classified information is official information which requires protection in the interest of national security and which has been so designated in accordance with Executive Order (EO) 12356. Classified defense information is classified TOP SECRET, or CONFIDENTIAL

Information subject to the Privacy Act of 1974: The Privacy Act of 1974 requires protection of systems of records by prohibiting unauthorized access to records containing unclassified personal data. AR 340-21, The Army Privacy Act Program, implements the Privacy Act in the Army and defines “personal data." Your Social Security Account Number (SSAN) is considered to be "personal data" and any form or record which contains your SSAN will be protected.

For Official Use Only information: This is unclassified official information of a sensitive nature which must be protected against unauthorized public release. FOUO information is defined in AR 340-17. An unclassified examination will be marked FOUO because even though it is unclassified, it requires protection from unauthorized disclosure.

Logistical and financial data: This data includes any unclassified information relating to the accounting and control of Army assets and resources. This "economically valuable data" is subject to theft, fraud, misappropriation, and misuse. Computer-related crime is big business; perhaps as high as $5 billion per year Included in this category is information relating to the control, accounting, and disbursement of Army assets and resources, including:

Funds: Funds are money, like pay and allowances.

Supplies: Supplies are things like paper, pencils, gasoline, and ammunition that the Army uses to do its job.

Material: Material includes buildings, weapons, vehicles, communications equipment, and other “real property."

How can data be valuable? The Joint Uniform Military Pay System (JUMPS) computer keeps track of your paycheck. The computer is not actually handling money, but rather data relating to the accounting of that money. If you could break into the JUMPS computer and have it issue you a few extra paychecks, you could make yourself rich. Then, so you won’t get caught, you delete the records of those extra paychecks. The auditors will see that money is missing, but won’t be able to figure out why.

U.S. Army intelligence activities: Although most information which concerns U.S. Army intelligence activities is classified, there is some that is unclassified. Anything dealing with intelligence activities which is not classified or FOUO, must still be considered to be sensitive and must be protected. One example is Field Manual (FM) 34-60, Counterintelligence. This FM is unclassified,

but on the front cover there is a notice which restricts distribution to U.S. Government agencies “to protect technical or operational information."

Government contracts: Any unclassified information concerning current or future Government contacts, details of contract negotiations, or information regarding bids on Government contracts is sensitive and requires protection from unauthorized access. There have been enough cases of fraud and abuse in this area to clearly demonstrate the need to protect this information.

Command and control: Unclassified information concerning the commander’s command and control of his forces also requires protection. This includes information relating to personnel management, communications, and planning and directing operations. Running a division is hard enough without having to worry about somebody erasing all the information about assignments of new personnel.

Mission-essential information: Mission-essential information is a kind of “catch-all:” any unclassified information, not in one of the above categories, which the commander considers to be of utmost importance to the units ability to perform its mission. In this category the commander can include any information that he thinks requires some degree of protection against unauthorized disclosure, modification, or destruction.

Part H: Responsibilities and Appointments

Security is everybody’s responsibilities, but AR 380-19 requires formal assignment of authority and responsibility. This requirement is intended to make sure that there is one specific individual who is responsible for the security of an identified computer or group of computers. Formal assignment implies that these individuals must be appointed in writing. A clearly defined structure of ISS personnel will assist the commander in implementing the units computer security program.

The specific duties and responsibilities of these designees will depend on the level of command, the type of computer used, and the geographic location. In general ISS personnel are responsible for making sure:

The unit’s computers are operated within the requirements of AR 380-19.

Adequate computer security policies, safeguards, and procedures are developed, applied and maintained.

Written instructions concerning computer security are developed and provided to all computer users.

All computer users receive periodic computer security awareness training.

Part I: The Commander

Computer security starts with the commander. The unit commander, along with all his other responsibilities, has overall responsibility for the security of all computers in that unit Paragraph 1-6c, AR 380-19, sums up the commander’s responsibility for computer security very well;

"Commanders and managers implement the computer security program in their command or activity to ensure that systems are operated within the requirements of this regulation."

NOTE: "Manager," as used here, refers to a civilian in charge; it does not mean the "security manager."

Computer security is a "command responsibility," but not only a company or battalion commander is responsible for computer security. Anybody in a command, management, leadership, or supervisory position is responsible for this security.

What does "command responsibility" mean? According to paragraph 1-3, FM 101-5, The commander alone is responsible for all that his unit does or fails to do. He cannot delegate this responsibility. The final decision, as well as the final responsibility, remains with the commander."

The commander has overall responsibility, but he can't personally do everything and must rely on certain people in the unit to assist him in fulfilling these duties. Commanders routinely delegate certain tasks to subordinates, such as appointing a security manager to take care of classified material. For computer security, the commander or manager appoints individuals to the following positions to assist him:

Part J: Security Officers

The Information System Security Officer (ISSO). The ISSO takes care of the commander's computers and their related security requirements, just like the security manager takes care of the commanders classified material and its related security requirements.

The ISSO is clearly a key position in the unit, however, AR 380-19 does not specify a minimum rank or grade requirement for an ISSO. Anybody can be appointed as an ISSO, as long as the commander considers that individual to be qualified to do the job. And, of course, the ISSO must have an appropriate security clearance.

Paragraph 1 -6d(3), AR 380-19, says that "For each computer or group of computers, there will be an ISSO appointed by the commander or manager of the activity operating the computer. The same ISSO may be appointed for multiple computer systems, particularly in the environment of small computers, local area networks, or small systems ....."

The Terminal Area Security Officer (TASO). The commander or manager may also have to appoint a TASO, or several TASOs. Paragraph 1-6d(5), AR 380-19, says that "For each terminal or contiguous group of terminals not under the direct control of an ISSO, there will be a TASO."

A terminal, is "a device in a computer system that performs input or output operations." Terminals are connected to a computer system by a "communications channel" along which signals may flow, like a telephone line or a cable. Terminals are used by computer users to enter (input) data into the computer and to get (output) data out the computer.

"Remote" terminals are located away from the computer itself, in a different room in the building, in a different building, or on a completely different installation. There might be a single remote terminal, or a "contiguous group" of two or more remote terminals located in the same area. These remote terminals are not under the ISSOs direct control; the ISSO can't control access to these remote terminals and a TASO is required for each terminal area.

Like for the ISSO, AR 380-19 does not specify a minimum rank or pay grade requirement for a TASO. Anybody the commander considers to be qualified and has an appropriate security clearance is eligible to be a TASO.

ISS Personnel Hierarchy. Within a unit there is a chain of command which begins with the soldier and ends with the commander, with squad leaders and platoon leaders between the soldier and commander. Operational orders come from the commander to the soldier through this chain of command. If a soldier has a problem, he usually goes through the chain of command; squad leader, platoon leader, and then commander.

The ISS responsibilities and appointments which are required by AR 380-19 result in a parallel chain of command for ISS personnel. The commander uses this parallel ISS chain of command for any actions or requirements which relate to ISS. A commanders computer security policies get to the individual computer users through this chain; commander, ISSO, TASO, and then individual user.

Within this parallel chain, the ISSO supervises the TASOs and the TASOs supervise the individual users, for anything related to computer security. And, if a computer user has a computer security problem or question, he usually goes through this ISS chain of command; TASO, ISSO, and then commander.

Most ISSOs and TASOs are appointed to these ISS positions as an “additional duty," and fall into both chains of command.

A battalion might adopt a policy on ISS appointments wherein an ISSO is appointed for the battalion and for each company, and TASOs are appointed for each of the platoons, squads, or sections which have PCs.

Lesson 1

PRACTICE EXERCISE

The following material will test our grasp of the material covered in this lesson. There is only ONE correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. What are the four ISS sub-disciplines? ________________________, ______________,________________, and ____________________.

2. Which of the three major security objectives are you meeting by safeguarding a classified Document from unauthorized disclosure?
________________________________.

3. Sensitive Defense Information includes classified information. What other information is included?
______________________________.

4. In which type of Sensitive Defense Information is your Social Security Account Number SSAN) included?
______________________________.

5. A unit uses PCs and word processors to process unclassified and classified (up to SECRET) information. Which level of security clearance must the unit ISSO have?
________________________________.

LESSON 1

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM CORRECT ANSWER AND FEEDBACK

1. COMSEC, ELSEC, TEMPEST, and COMPUSES (in any order) (pages 1-4).

2. Confidentiality (page 1-5).

3. Unclassified-sensitive information (pages 1-5).

4. Information subject to the Privacy Act of 1974 (pages 1-5 and 1-6).

5. At least SECRET (page 1-8).

LESSON 2

THE THREATS TO ARMY COMPUTERS AND SENSITIVITY DESIGNATIONS

CRITICAL TASK: NONE.

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn the various threats to computers and the sensitivity designations assigned to Army computers.

TERMINAL LEARNING OBJECTIVE:

ACTIONS: Identify the three major types of threats to Army computers, define the threats to Army computers, list and define the sensitivity designations, and assign a computer to the correct sensitivity designation based on the information which will be processed on it.

CONDITIONS: You will be given narrative information and extracts from AR 380-19.

STANDARDS: You will be able to provide advice and assistance to your commander and other units in recognizing the threats to computer security and in assigning computers to a sensitivity designation.

REFERENCES: The material contained in this lesson was derived from the following publications:

AR 380-5
AR 380-19
AR 380-67
DOD 5200.22-M
FM 19-30

Part A: The Threats to Army Computers

Field Marshal A. V. Suvorov (1729-1800) said “we must know the enemy if we are to Protect ourselves from him.” If we are to protect our Army computers, we must know the threats to these computers. A threat is any person, thing or event which can damage or destroy a computer or the information it processes. There are three major types of threats to our computers, environmental, foreign intelligence, and human.

The Environmental Threat. The world is a dangerous place for our computers, which face several environmental enemies:

Natural Events: Tornadoes, floods, windstorms, rain, snow, and earthquakes.

Fire: A fire will bum your building, your computer and your floppy disks. The sprinkler system will get what the fire doesn't.

Power: If the power goes out, your computer won't work. If lightning hits the power line, the "power surge" will "fry" your computer.

Temperature Extremes: The units which took PCs to Saudi Arabia on Operation Desert Shield/Desert Storm experienced temperature extremes of 125 degrees or more. In this heat, some computers don't work very well!

The Foreign Intelligence Threat. Although there is very little hard evidence of actual or attempted computer espionage, we cannot assume that no attempts have been made.

Dr. Brotzman, the former Director of the National Computer Security Center (NCSC), believes that U.S. computers are too lucrative a target for foreign intelligence agencies to ignore. Dr. Brotzman commented, "Considering how must fun the bad guys could have on U.S. computers, if they ain't having at them, they're a lot dumber than we think they are."

The foreign technical threat: We live in a computer world. We can easily imagine highly-trained, technical agents of other countries using state-of-the-art computers to break into US defense-related computers.

The foreign HUMINT threat: Foreign intelligence agencies are not limited to using only "technical" means to attach US computers. They will use all means of attack, to include traditional methods of espionage and subversion.

The Human Threat. The basic threat to Army computers is the human threat; most computer security problems are human-related.

The thief: The Federal Bureau of Investigation (FBI) estimates that the annual cost of computer-related crime in the US is somewhere between $1.5 billion and $5 billion. The National Crime Information Center reports that more than 137,000 PCs, worth more than $154 million, were stolen in 1986.

The "hacker." The media has made the most of the exploits of "hackers;" teen-age whiz kids equipped with a PC and "having a little harmless fun." In the hacker ethic, "any weakness in an Automated Data Processing (ADP) system can and should be exploited." However, "technological trespassing" into a U.S. defense-related computer goes beyond "harmless fun."

The authorized user. Hackers, tornadoes, and foreign intelligence may be the least of our worries. It is said that we all know computer thieves, because we work with them. For example, disgruntled employees sometimes sabotage computers. However, the biggest threat comes from employees who have no intention of committing a crime. Through accident or carelessness, files get deleted, classified information gets copied onto an unclassified disk, and coffee gets spilled on a computer.

Part B: Methods of Attack.

The following are some common methods of attack:

Insider misuse. Some of the most serious breaches of security are performed by insiders misusing their access authorizations. This is another reason why total security is unachievable. Although a user's rights can be contained, they can never be so constrained as to preclude any misuse.

Social engineering. The attacker uses lies and deception to con the victim into providing information (e.g., passwords) that facilitates an attack. Strong technical safeguards can be useless against this form of attack.

Password cracking: Many passwords are easily guessed or vulnerable to systematic attack. These attacks are typically launched with the aid of a dictionary and password cracking program. First the attacker acquires a file of encrypted passwords. Then the cracking program is used to encrypt all of the words in the dictionary along with commonly chosen passwords until a match is found in the encrypted password file.

Key cracking. If encryption keys are not sufficiently long, they can be systematically broken by trying all possible keys until the correct one is found. Even keys that are long enough to withstand a brute force attack can be cracked if he random number generator used to create keys is not sufficiently good or if the cryptosystem has protocol failures or other weaknesses. In some cases, keys have been broken within a few minutes.

Sniffers. "Sniffer" programs, installed on network nodes, intercept packets traversing the network and ferret out login IDs and passwords, credit card numbers, or messages containing certain keywords. This information is stored in a file, where it can be read by or transmitted back to the owner of the program.

IP Spoofing. This involves forging the Internet Protocol (IP) address of a trusted host in order to establish a connection with a victim machine. One method floods the trusted host with connection requests and then, while the host is recovering, sends packets that forge the node's IP address. The forged packets may contain data that allow the attacker to gain privileged access on the victim machine.

Injecting viruses, Trojan horses, time bombs, and other malicious code. Malicious code is injected into a target system through a disk or computer network. The code could alter or destroy data or cause other types of mischief.

Exploiting weaknesses in operating systems, network protocols, and applications. In general, any system vulnerability can be exploited to form an attack. Depending on the weaknesses, such attacks may effectively circumvent access controls and encryption, allowing access to plaintext data without the need to crack passwords or encryption keys. An intruder may be able to download tens of thousands of credit or calling card numbers at a time. Weaknesses are often found in configuration settings and parameter checking.

Part C: Sensitivity Designations

In information security, protective measures are based on the classification of the information; the higher the classification of the information, the more protection you must give that information. The amount of protection required for a computer is based on the computer. Each Army computer is designated, or assigned a sensitivity designation, based on the highest classification or sensitivity of information which will be processed by that computer.

Paragraph 2-2a, AR 380-19, says "AIS will be designated, based on the highest classification or sensitivity of information processed." Each Army computer, word processor, and any other computer will be designated or "assigned a sensitivity designation." This designation, like a classification marking, will tell you how much security you will have to provide that computer.

This sensitivity designation is based on the sensitivity of the information processed; it has nothing to do with the size, type, or model of the computer. We will go through the sensitivity designations, starting at the highest level and ending at the lowest level of sensitivity.

Classified Sensitive. Classified Sensitive is the highest sensitivity designation. A computer which processes any classified information will be designated Classified Sensitive One, Two, or Three as follows, based on the highest classification of information processed by this computer:

Classified Sensitive One (CS1): A computer will be designated CS1 if it processes sensitive compartmented information (SCI) or Single Integrated Operations Plan-Extremely Sensitive Information (SIOP-ESI).

Classified Sensitive Two (CS2): A computer will be designated CS2, if it processes TOP SECRET information.

Unclassified Sensitive. As the designation suggests, this applies to computers which process unclassified-sensitive information. As well as protecting classified information from unauthorized disclosure, we must also protect unclassified-sensitive information, such as FOUO information and information subject to the Privacy Act of 1974. Computers which processes any unclassified-sensitive information will be designated Unclassified Sensitive One or Two as follows, based on the highest sensitivity of information processed by this computer:

Unclassified Sensitive One (US1): A computer will be designated US1, if it processes any unclassified information which:

Involves intelligence activities.

Involves command and control of forces.

Is determined by the commander to be mission essential.

Unclassified Sensitive Two (US2): This designation also applies to computers which process unclassified-sensitive information. A computer will be designated US2, if it processes any unclassified information which includes:

Information subject to the Privacy Act of 1974.

FOUO information.

Logistical or financial data.

Government contract information.

Nonsensitive. In rare cases, an Army computer may be designated Nonsensitive, provided it does not fall into any of the above sensitivity designations. Very few Army computers are designated Nonsensitive because most Army computers process either classified or unclassified-sensitive information and are designated at least US2.

A computer can be designated as Nonsensitive only if it processes no classified information and no unclassified-sensitive information. It can process only what is defined as “public information.” “Public information” is information that is freely available to the general public. There are no restrictions on the release of this information. The location of Fort Huachuca is “public information.”

All Army computers will be designated CS1, CS2, CS3.1, US2, or Nonsensitive, based on the highest classification or sensitivity of information processed. An Army computer is probably not going to process only one kind of information. If a computer processes information that is in different sensitivity levels, it will be designated at the highest level. This is like determining the overall classification of a document; that’s based on the highest classification of information in the document.

EXAMPLE: A computer will be used to process SECRET information (which is CS3) and TOP SECRET information (which is CS2). This computer will be designated CS2. Of the two types of information processed, TOP SECRET (CS2) is the highest classification.

LESSON 2

PRACTICE EXERCISE

The following material will test your grasp of the material covered in this lesson. There is only ONE correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item Incorrectly, study again that part of the lesson which contains the portion involved.

1. The Foreign Intelligence Threat is one of the threats to Army computers. One type of Foreign Intelligence Threat is the "technical" threat What is the other type of Foreign Intelligence Threat?
   ________________________________.

2. Of the three threats, which is the basic threat?
   ________________________________.

3. A computer will be used to process FOUO information. Which sensitivity designation must be assigned to this computer?
   ________________________________.

4. A computer will be used to process SECRET information and CONFIDENTIAL information. Which sensitivity designation must be assigned to this computer?
   ________________________________.

5. Each Army computer is assigned a sensitivity designation. What is this sensitivity designation based on?
   ________________________________.

6. An Army computer can be assigned a sensitivity designation of "Nonsensitive" only if it processes what kind of information?
   ________________________________.

LESSON 2

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM CORRECT ANSWER AND FEEDBACK

1. The Foreign Intelligence “HUMINT” treat (page 2-2).

2. The Human threat (page 2-2).

3. Unclassified Sensitive Two (US2)(page 2-4).

4. Classified Sensitive Three (CS3)(page 2-4).

5. It is based on the highest classification or -sensitivity of information processed (page 2-5).

6. Public Information (pages 2-5).

LESSON 3

SECURITY PROCESSING MODES AND ACCREDITATION

CRITICAL TASK: NONE.

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn the various security processing modes and the computer accreditation process.

TERMINAL LEARNING OBJECTIVE:

ACTIONS: Identify and define the security processing modes, define accreditation, explain accreditation requirements for Army computers, and Identify the Designated Accreditation Authorities (DAA).

CONDITIONS: You will be given narrative information and extracts from AR 380-19.

STANDARDS: You will be able to determine the required security processing mode for Army computers, and request an accreditation from he proper DAA.

REFERENCES: The material contained in this lesson was derived from the following publications:

AR 380-19

Part A: Security Processing Modes

The security processing mode of an Army computer will be determined based on the classification or sensitivity and formal categories of data, and the clearances, access approval, and need-to-know of the users of the system. The available or proposed security features of the system are not relevant in determining the actual security mode. All Army computers will be accredited to operate in one of four security processing modes.

Part B: Explanation of terms

Formal categories of information: Information, such as SCI and NATO classified, which require written approval for access.

Formal access approval: Documented (written) approval for access to a particular category of information, such as SCI or NATO classified.

Part C: The four security processing modes

Dedicated security mode: A mode in which all users have the required security clearance, formal access approval, and a need-to-know for all information processed by the system.

EXAMPLE : A computer is used to process classified (up to SECRET) information, including NATO SECRET. In this mode all users must have at least a SECRET clearance, all users must have formal access approval for NATO SECRET, and all users must have a need-to-know for all information processed.

Systems high security mode: A mode n which all users have the required security clearance and formal access approval, but do not have a need-to-know for all information processed.

EXAMPLE: A computer is used to process classified (up to SECRET) information, including NATO SECRET. In this mode all users must have at least a SECRET clearance and all users must have formal access approval for NATO SECRET. However, not all users have a need-to-know for all information processed.

Partitioned security mode: A mode in which all users have the required security clearance. However, not all users have formal access approval and a need-to-know for all information processed by the system.

Multilevel security mode: A mode in which not all users have the required security clearance for all information processed by the computer.

Part D: The Accreditation Document/Security Plan

Accreditation is authorization for a computer to process information at one of the sensitivity levels, in a particular security processing mode, using a prescribed set of security safeguards.

Appendix C, AR 380-19, provides the sample format for the Security Plan/Accreditation Document" which describes that prescribed set of security safeguards. The document/plan is a detailed description of the system (make, model, location, and use; sensitivity level; information to be processed; and the security processing mode) and the security safeguards which will protect both the computer and the information processed.

The document/plan is normally prepared by the ISSO and is forwarded to the DAA along with the commanders request for accreditation. The DAA will review the document/plan to determine if security is adequate and if the computer will be accredited. If the DAA decides that security is NOT adequate, he will not accredit the system, and will return the document/plan with guidance on what must be done to improve security.

Among the security safeguards which must be described in the document/plan, is how classified and unclassified-sensitive information will be protected from unauthorized exploitation. Before the DAA will accredit the system, safeguards and procedures must be developed to protect this information from unauthorized disclosure, manipulation, and destruction by an unauthorized person, like a foreign intelligence agent.

NOTE: The accreditation document contains information of value to an unauthorized intruder. At a minimum, it will be safeguarded as FOR OFFICIAL USE ONLY.

Part E: Accreditation

Our next topic of discussion is a very important part of computer security. The term "accreditation" is synonymous with "approval to operate." In the Army we must have this approval to operate before we can use a computer to process any classified or unclassified-sensitive information. This lesson will introduce you to accreditation, to the Army's accreditation requirements, and the accreditation process.

Why accreditation? Accreditation is the key to security. Accreditation can be thought of as "an application for a license to operate," like getting a driver's license to operate a motor vehicle, and the reason for requiring approval to operate a computer is the same mason you have to have a drivers license.

Before you can drive a car you have to have a license. To get a license you have to show the licensing authority (like the Department of Motor Vehicles) that you can operate a car in compliance with the rules of the road. If you didn't need a drivers license, and anybody could just buy a car and hit the road, the number of accidents would skyrockets!

Before you can operate an Army computer you have to have an accreditation. To get an accreditation you have to show the accreditation authority that you can operate that computer in compliance with the rules of computer security, as specified In AR 380-19. If you didn't need an accreditation and any unit could just get a computer and start processing classified information, the number of compromises would skyrocket!

Accreditation is a formal declaration by the DAA that a computer is authorized for operation. Accreditation is approval for it to process information at one of the sensitivity levels, using a prescribed set of security safeguards. Basically, accreditation requires that a unit develop security safeguards, submit them for approval, and begin processing after approval is granted.

Part F: Initial Accreditation

Before we can use a new computer to process any classified or unclassified-sensitive information, it must be accredited. That's initial accreditation, and that's what Paragraph 2-3a(10), AR 380-19, means when it states, "Before operation, each computer (except those computers which are designated as Nonsensitive) will be accredited under a set of security safeguards approved by the DAA." The term "before operation" means that the computer cannot be used to process any classified information or any unclassified-sensitive information until the DAA has formally authorized this processing in writing.

Part G: Accreditation Level

Each computer is designated based on the highest classification or sensitivity of information which is processed by that computer. Accreditation is authorization to process information at one of the sensitivity levels. A sensitivity designation, like CS3 or US1, is also referred to as a "sensitivity level."

If a computer processes information in different sensitivity levels, the computer will be designated and accredited at the highest sensitivity level of any information that is to be processed on it.

EXAMPLE: A computer processes CS3 information, US1 information, and US2 information. This computer will be designated as CS3, and will be accredited at the CS3 level. Accreditation at the CS3 level means the computer is approved to process CS3 information and any information in a lower sensitivity level; US1, US2, and Nonsensitive.

WNINTEL: A computer which processes any data controlled under the caveat “WNINTEL" (Warning Notice - Intelligence Sources or Methods involved), will have that additional identifier associated with the assigned sensitivity designation.

EXAMPLE: A computer which will be used to process SECRET - WNINTEL information will be designated "CS3 - WNINTEL" and will be accredited at the "CS3 - WNINTEL” level.

Part H: Designated Accreditation Authorities

Accreditation is approval to operate, and the individual who gives this approval is the “designated accreditation authority” or “DAA”. The DAA for an Army computer is determined by the sensitivity level at which the system will be accredited.

Part I: Explanation of Terms

Before you begin reading the information about the DAA, read the following terms and make sure that you understand what each term means.

Designated accreditation authority (DAA): A senior management official who has the authority and responsibility to accredit (approve the operation of) an Army computer, based on a prescribed set of security safeguards.

MACOM commanders: The MACOM commanders are the Commanding Generals of the Army MACOMs (major commands). MACOMs include U.S. Amy Forces Command (FORSCOM); U.S. Army European Command (EUCOM); Training and Doctrine Command (TRADOC), and U.S. Army Intelligence and Security Command (INSCOM).

Senior executive service (SES) personnel: Civilian personnel In civilian pay grades GS-16, GS-17, and GS-18.

Position of command: Command positions include brigade commander, division commander, and corps commander. The position of “deputy commander” is also considered a command position.

Principle staff officer. A division or corps commander has a staff of officers who assist him in certain functions. The principle staff officers are the Chief of Staff (directs the staff); G1 (personnel); G2 (intelligence); G3 (operations and training); G4 (logistics); and G5 (Civil Affairs).

Delegation of accreditation authority: The action by which an accreditation authority assigns part of his authority to a subordinate.

Part J. Classified Sensitive One (CS1)

A computer which processes SCI or SIOP-ESI will be designated CS1 and must be accredited. Accreditation of a computer to process at the CS1 level is a special situation. These systems must comply not only with AR 380-19, but with DOD, Central Intelligence Agency (CIA), and other policies as well. Therefore, the DAA for CS1 will not be discussed.

Part K: Classified Sensitive Two (CS2)

A computer which processes TOP SECRET information will be designated and accredited CS2. MACOM commanders are the designated accreditation authorities for CS2 computers.

EXAMPLE: If you were assigned to the 18 Airborne Corps at Fort Bragg, North Carolina, your CS2 DAA would be the Commanding General (CG) of FORSCOM.

Delegation of CS2 accreditation authority: AR 380-19 authorizes delegation of CS2 accreditation authority for systems operating n the dedicated system high or partioned mode MACOM Commanders may delegate, in writing, CS2 accreditation authority to certain individuals in the MACOM. These individuals are general officers and civilian senior executive service (SES) personnel. Delegation may be by name or by established position titles.

Part L: Classified Sensitive Three (CS3)

A computer which processes SECRET or CONFIDENTIAL will be designated and accredited CS3. The MACOM commanders are also the designated accreditation authorities for CS3.

Delegation of accreditation authority: Like for CS2, the MACOM commander is authorized by AR 380-19 to delegate CS3 accreditation authority. The MACOM commanders may delegate, in writing, CS3 accreditation authority to certain individuals in the MACOM. Those individuals are colonels (COL-06) and civilians (GM-15/GS-15) who are occupying a position of command or principal staff officer at an installation or general officer command.

Part M. Unclassified Sensitive One (US1) and Unclassified Sensitive Two (US2)

US1 and US2 computers have the same DAA. First individuals authorized to accredit Classified Sensitive (CS1, CS2, and CS3) computers are also authorized to accredit US1 and US2 computers.

EXAMPLE: A MACOM commander can accredit US1 and US2 computers. Any generals or SES personnel who have been delegated CS2 accreditation authority can accredit these computers. And, any colonel or GM-15/GS-15 who has been delegated CS3 accreditation authority can also accredit these computers.

Delegation of US1 and US2 accreditation authority: The MACOM commanders may also delegate, in writing, US1 and US2 accreditation authority to certain individuals in the MACOM. These individuals are lieutenant colonels (LTC-05) aid civilians (GM-14/GS-14).

Part N. Nonsensitive

No accreditation is required for a computer which has been designated as Nonsensitive. However, this designation must be approved in writing by an appropriate US1 or US2 accreditation authority. The reason for this approval is to make sure that the computer is in fact Nonsensitive. Since accreditation is not required, some units might be tempted to designate all their computers Nonsensitive, just to get out of having to worry about accreditation.

To finish our discussion of the designated accreditation authorities, there are three things to note:

No further delegation: Except for the delegation discussed above, accreditation authority may not be further delegated. For example, if the MACOM commander delegates CS2 authority to a general who is a division commander, the division commander may not pass this authority along to a second general, like the assistant division commander. Only the MACOM commander s authorized to delegate accreditation authority.

Delegation in writing: Delegation of accreditation authority must be in writing, such as in a memorandum signed by the MACOM commander. The delegation of accreditation authority can be by name or by position title. A MACOM commander can issue a memorandum delegating CS3 accreditation authority to a Colonel by name o to a Colonel by his position title of Commander, 2d Brigade, 52d Infantry Division.

Also DAA for any lower levels: The DAA for a particular sensitivity level is also authorized to accredit a system at any lower sensitivity level. For example, a DAA for CS3 is also a DAA for US1 and US2, and may approve the designation of Nonsensitive. This holds true for all the DAA for all the sensitivity levels.

Part O: Preparing the Accreditation Document/Security Plan

You request a security clearance by filling out and submitting a bunch of forms to the United States Army Personnel Central Clearance Facility (CCF), including a Standard Form (SF) 86. The SF 86 gives personnel at CCF enough information about you to decide if you can be trusted with a security clearance and access to classified information. Accreditation is authorization for a computer to process information at a particular sensitivity level, using a prescribed set of security safeguards. Appendix C, AR 380-19 provides the sample format for the “Accreditation Document/Security Plan” which describes that “prescribed set of security safeguards.”

The accreditation document/security plan is just that; a very detailed description of exactly what the unit plans to do with its computers and how it intends to protect those computers and the information they will process from unauthorized disclosure, modification, and destruction. It describes the computer and the security safeguards which will protect the computer and the information processed.

The accreditation document/security plan is normally prepared by the ISSO, and is forwarded to the DAA along with the commanders request for accreditation. The DAA will review the accreditation document/security plan to determine if security is adequate and if the system win be accredited. If the DAA decides that security is T adequate, he will not accredit the computer and will return the accreditation document/security plan with guidance on what must be done to improve security.

NOTE: The accreditation document/security plan contains information of value to an intruder. It describes the security safeguards used to protect the computer and will give the intruder information which he can use to defeat those safeguards. Sometime an accreditation document/security plan will be classified. If unclassified, it will be safeguarded as FOR OFFICIAL USE ONLY.

Part P: Reaccreditation

A computer is accredited to operate using a prescribed set of security safeguards which are described in the accreditation document/security plan. The safeguards which will work for a computer in one location probably won't work for that same computer in another location. Moving a computer changes the security situation.

If there are any changes which will affect security, the ISSO must initiate a reaccreditation. The purpose of the reaccreditation is to determine how the change will affect security, and what additional or different security safeguards must be developed to maintain adequate security of the system. Then, the accreditation document/security plan is redone and submitted to the DAA for approval for continued accreditation. There are three situations which may affect security and may require reaccreditation:

Equipment change: The first situation is an equipment change. An equipment change is when an accredited computer is replaced with a different computer, or if any computer equipment is added to the computer. A different computer will probably mean some change in security procedures, and the ISSO must consider what must be done. If the replacement computer is the same exact model, there is probably no security impact, but the DAA must still be notified.

Physical change: A physical change is a change to the building or a change in the location of the computer. If the engineers remove walls or add windows to the building, that's going to affect security. And, a different location means different physical security. Just moving the computer from one desk to another in the same office probably doesn't require reaccreditation, but again the DAA must be notified.

Increase in sensitivity level: Accreditation is authorization to process at a certain sensitivity level. An increase in sensitivity level will require reaccreditation, in most cases. An increase from US2 to US1 won't require reaccreditation, in most cases. An increase from US2 to US1 won't require much more security, but an increase from US1 to CS2 is a different story. Any time a computer which is accredited to process at a particular sensitivity level will be used to process information "in a higher level, reaccreditation must be considered and the DAA notified.

Reaccreditation: Reaccreditation is required after three years. This is not a "maybe," like for the other situations; this must be done. There is a need for periodic formal review of a computer system's security safeguards and procedures, and reaccreditation is also required on a scheduled basis; three years after accreditation.

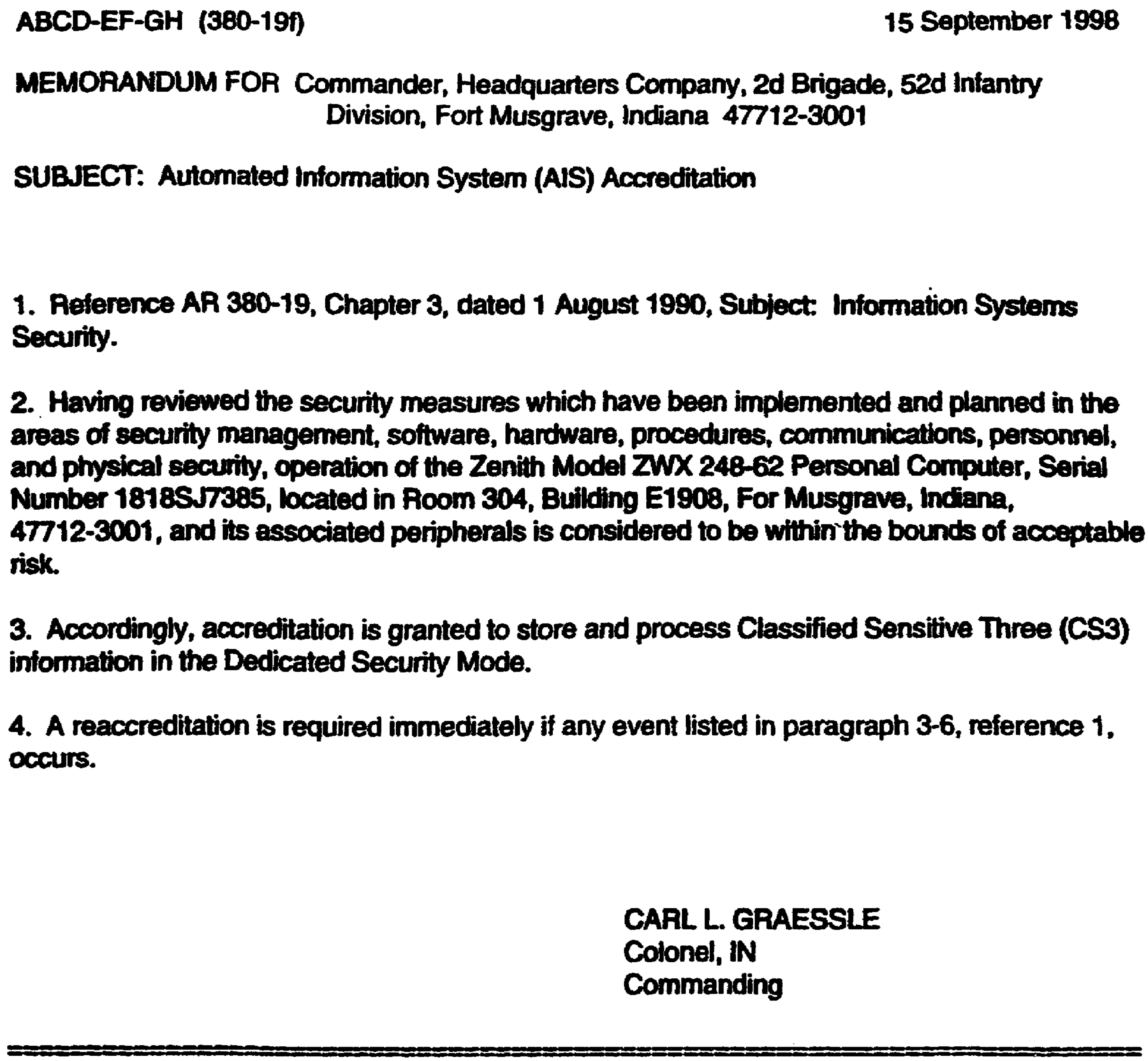
Reaccreditation after three years is mandatory. In case of the other changes, the ISSO should first contact the DAA and find out if reaccreditation is required. The final decision on reaccreditation will be mad by the DAA. The rule is “when in doubt, contact the DAA” The DAA would much prefer an ISSO to notify him of any and every change, no matter how minor, than have the ISSO notify him that here was a major security problem as a result of some change which had an impact on security.

Part Q: The Accreditation Statement

The difference between authorized access to classified information and compromise is a DD Form 873, Certificate of Clearance and/or Security Determination, issued by CCF. The difference between your computer being accredited and you being in violation of AR 380-19, is an accreditation statement issued by the DAA. Accreditation is effective when the DAA issues a formal, dated, statement of accreditation. An accreditation statement is issued on initial accreditation and upon reaccreditation.

Figure 3-1, AR 380-19, provides the format for the accreditation statement, and example of which is shown on the following page.

The Department of Defense Security Institute (DoDSI) reports that one of the leading computer security problems is “not operating as documented.” Accreditation is not a unique Army procedure; most Government agencies have a requirement for some kind of written authorization to use a computer, and not operating in accordance with this authorization is a problem the DoDSI finds frequently and in every agency.



ABCD-EF-GH (380-19f) 15 September 1998

MEMORANDUM FOR Commander, Headquarters Company, 2d Brigade, 52d Infantry
Division, Fort Musgrave, Indiana 47712-3001

SUBJECT: Automated Information System (AIS) Accreditation

1. Reference AR 380-19, Chapter 3, dated 1 August 1990, Subject: Information Systems Security.

2. Having reviewed the security measures which have been implemented and planned in the areas of security management, software, hardware, procedures, communications, personnel, and physical security, operation of the Zenith Model ZWX 248-62 Personal Computer, Serial Number 1818SJ7385, located in Room 304, Building E1908, For Musgrave, Indiana, 47712-3001, and its associated peripherals is considered to be within the bounds of acceptable risk.

3. Accordingly, accreditation is granted to store and process Classified Sensitive Three (CS3) information in the Dedicated Security Mode.

4. A reaccreditation is required immediately if any event listed in paragraph 3-6, reference 1, occurs.

CARL L. GRAESSLE
Colonel, IN
Commanding

Figure 3-1, AR 380-19
Sample format of an accreditation statement

The preceding illustration is an example of an accreditation statement. This statement was issued by the Commander of the 2d Brigade, 52d Infantry Division.

One of the things you are being trained to do is to conduct a security inspection. If you are inspecting a unit's computer security program, you would ask for the accreditation statements for their computers. Then, you would have to compare the accreditation statements against the actual operation to make sure that the unit was operating its computers like, it was authorized to operate them. In the accreditation statement, the DAA states what the unit is authorized to do, and if they are doing anything else, that's "not operating as documented." Along with the statement, you would also ask the ISSO for the accreditation document/security plan which was used to request this accreditation. The following are some common problems and areas that must be checked.

The date: The statement must be dated to show the date when accreditation is effective. And, the date on the statement must be less than three years old.

The unit: The statement must be issued in the unit that has the computer. The line in the statement which starts "MEMORANDM FOR" shows which unit the statement was issued to. If the ISSO from Charlie Company, 2/16" Infantry showed you this statement, that would be a problem because this statement was issued to a different unit.

The computer The unit must be using their computers exactly as authorized. The statement authorizes them to use a specific computer, in a specific location, to process at a specific sensitivity level:

The actual computer must be the same as the authorized computer, by brand, type, model and serial number. The computer they are using must be the same one that is identified in the statement. You must also check the accreditation document/security plan to make sure the unit is using only the authorized "associated peripherals," such as printers; modems, and any other computer equipment. The computer and all associated peripherals must be identified (by brand, type, model, and serial number) in the accreditation document/security plan.

The actual operating location must be the same as the authorized operating location; room, building, and post.

The actual level of processing must not be higher than the authorized level of processing (accreditation level), like CS3 or US1.

The signature: The statement must be personally signed by the DAA. The statement may not be signed "for the DAA" by another individual. The individual who signed it must be the individual whose name is in the signature block. The signature must be original and not a rubber stamp.

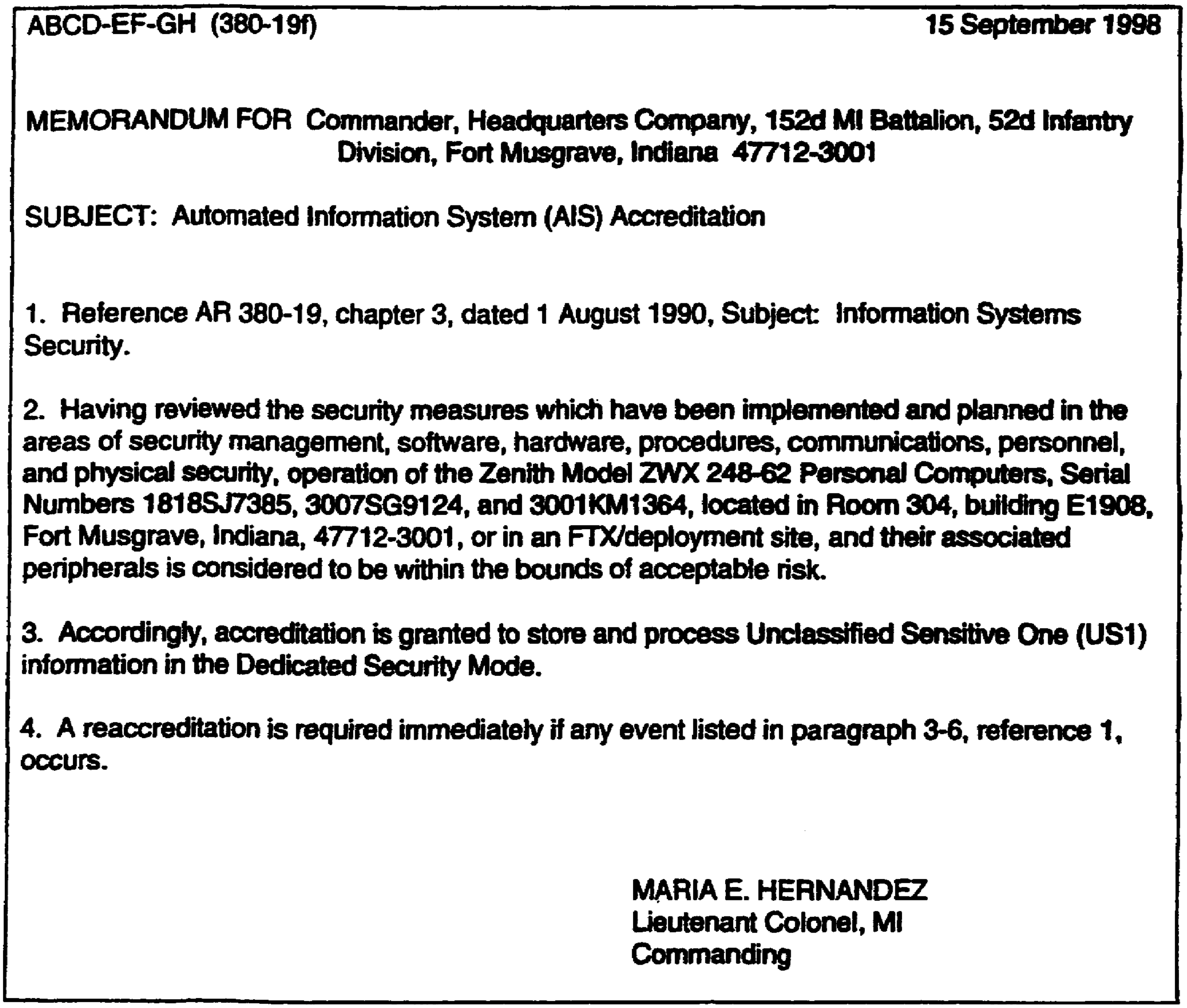
The signature block: The individual whose name, rank, branch, and position are typed in the signature block must be a DAA. On occasion, you might see a statement issued by somebody who isn't a DAA. This one looks good in that the Colonel is eligible to be a CS3 DAA; he's a "full" colonel, he's a commander, and he's in a division commanded by a general. But, you would have to make sure that he has been delegated this authority by asking the ISSO for the written delegation.

Copy of file: And finally, the unit must have an accreditation statement on file for each of its computers. The DAA and the ISSO are required to keep the statement, or a copy of the statement, on file. And a copy should also be on file in each office that has a computer.

Part R: Accreditation Variations

The accreditation statement shown at Figure 3-1 is a "basic" statement; it is for one PC operating in one location. However, accreditations are not limited to this basic situation and you may see a variety of situations addressed in accreditation statements.

Figure 3-2 is an example of an accreditation statement which is a variation from the basic accreditation. In this statement, the DAA approves the operation of three PCs in garrison, and in the field. These are two accreditation variations which you are likely to encounter.



ABCD-EF-GH (380-19f) **15 September 1998**

MEMORANDUM FOR Commander, Headquarters Company, 152d MI Battalion, 52d Infantry Division, Fort Musgrave, Indiana 47712-3001

SUBJECT: Automated Information System (AIS) Accreditation

1. Reference AR 380-19, chapter 3, dated 1 August 1990, Subject: Information Systems Security.

2. Having reviewed the security measures which have been implemented and planned in the areas of security management, software, hardware, procedures, communications, personnel, and physical security, operation of the Zenith Model ZWX 248-62 Personal Computers, Serial Numbers 1818SJ7385, 3007SG9124, and 3001KM1364, located in Room 304, building E1908, Fort Musgrave, Indiana, 47712-3001, or in an FTX/deployment site, and their associated peripherals is considered to be within the bounds of acceptable risk.

3. Accordingly, accreditation is granted to store and process Unclassified Sensitive One (US1) information in the Dedicated Security Mode.

4. A reaccreditation is required immediately if any event listed in paragraph 3-6, reference 1, occurs.

MARIA E. HERNANDEZ
Lieutenant Colonel, MI
Commanding

Figure 3-2. Example Accreditation Statement Variation.

<u>More than one computer:</u> A Especially in the case of small computers, the DAA may include more than one computer in one statement, providing they will all be operating at the same sensitivity level, in the same location, and sing he same security safeguards.

<u>More than one location</u>: The DAA may accredit a computer to operate in more than one location. Many units use tactical computers which are designed to be used in the field. A tactical computer may be accredited for use in he garrison location and at a deployment site. For this computer, a move from garrison to a field site is an authorized move and rot a physical change which requires reaccreditation.

Part S: Interim Approval to Operate Before Accreditation

When we discussed initial accreditation, you found out that all computers must be formally accredited, in writing, before operation. Sometime, however, a unit might get a new computer and have to use it right away. For example, if a unit got a new computer the day it was leaving on Operation Desert Shield, they probably had a lot of stuff on the agenda besides computer security. Sometimes, operations must take precedence over security.

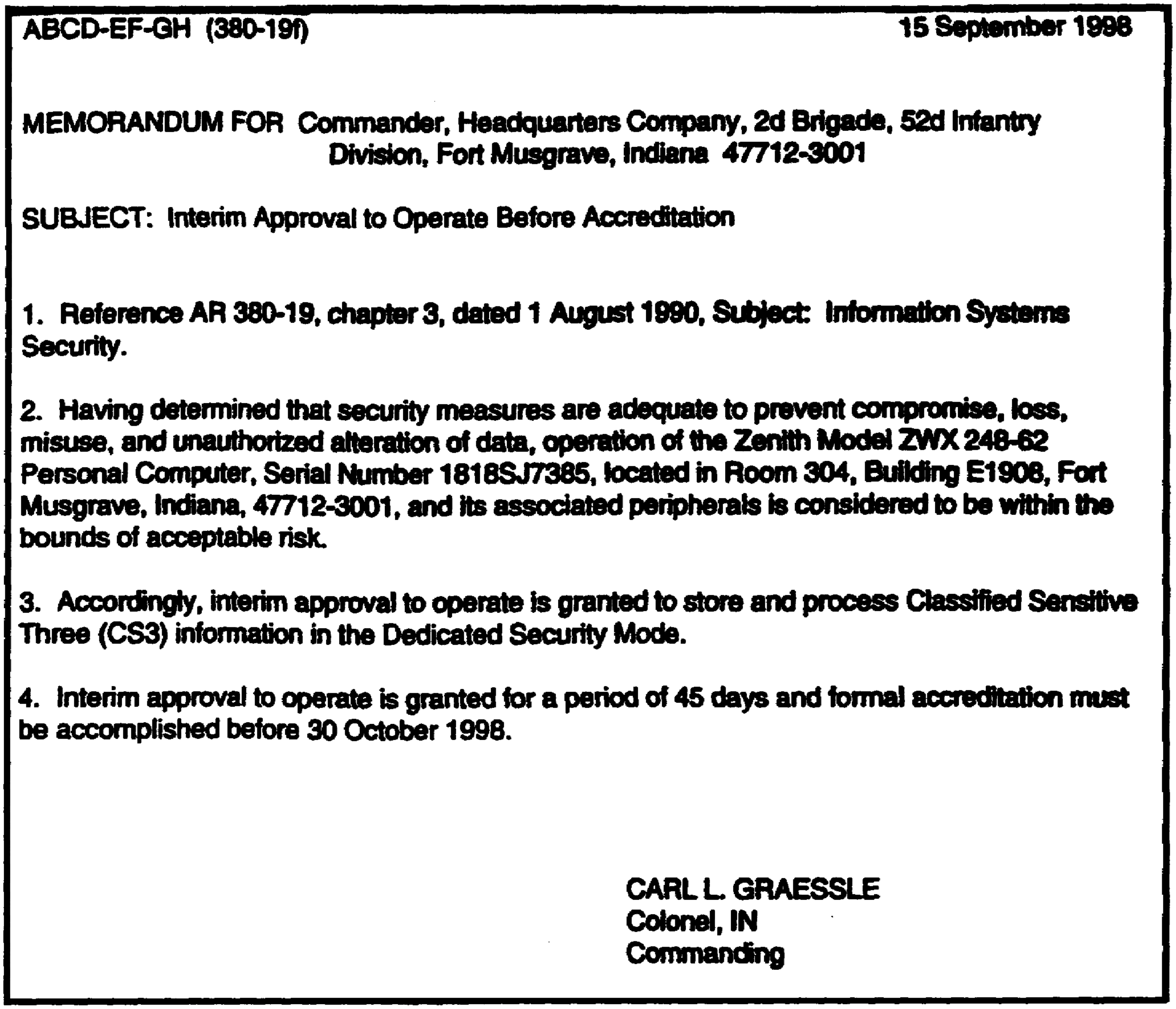
With such a situation in mind, AR 380-19 provides for "interim approval to operate before accreditation," which is a "temporary waiver of formal accreditation." This provision allows a new computer to be used before the accreditation document/security plan can be developed.

A DAA (and only the DAA) may grant interim approval to operate before accreditation, provided the following conditions are met.

Security survey: A security survey is performed and the DAA determines that there are adequate security measures to protect the information to be processed. If the unit has other computers already in use, existing security will probably be adequate.

Accreditation date: A definite accreditation date is established and agreed on. Both the unit and the DAA must agree that by a certain date formal accreditation must be completed, or the interim approval expires.

Specific time period: Interim approval will be for a specific time period, not to exceed 90 days. One additional 90-day extension may be granted, but the total length of interim approval will not exceed 180 days (Figure 3-3). That's the maximum time allowed by AR 380-19, but the DAA will probably grant interim approval for less time.



ABCD-EF-GH (380-19f) 15 September 1998

MEMORANDUM FOR Commander, Headquarters Company, 2d Brigade, 52d Infantry
Division, Fort Musgrave, Indiana 47712-3001

SUBJECT: Interim Approval to Operate Before Accreditation

1. Reference AR 380-19, chapter 3, dated 1 August 1990, Subject: Information Systems Security.

2. Having determined that security measures are adequate to prevent compromise, loss, misuse, and unauthorized alteration of data, operation of the Zenith Model ZWX 248-62 Personal Computer, Serial Number 1818SJ7385, located in Room 304, Building E1908, Fort Musgrave, Indiana, 47712-3001, and its associated peripherals is considered to be within the bounds of acceptable risk.

3. Accordingly, interim approval to operate is granted to store and process Classified Sensitive Three (CS3) information in the Dedicated Security Mode.

4. Interim approval to operate is granted for a period of 45 days and formal accreditation must be accomplished before 30 October 1998.

CARL L. GRAESSLE
Colonel, IN
Commanding

Figure 3-3. Example of an Interim Approval to Operate Before Accreditation

The above is an example of a written interim approval. Notice that the DAA has granted interim approval for only 45 days, not the maximum 90 days, and has specified the date this interim approval will expire.

Part T: Accreditation Problems and Corrective Action

So far in this lesson you have been introduced to the Army's accreditation requirements and to the accreditation process. You also found out that one of the leading computer security problems is not operating as documented. That's when the personnel in a unit are not operating their computers in compliance with AR 380-19 or within their accreditation. The following are common accreditation problems and how to "fix" those problems.

The first thing to understand is that the DAA is the only person who is authorized to issue an accreditation statement. Also, the DAA is the only person who is authorized to change the statement. If a unit receives a statement and there is an error in the statement, it must be returned to the DAA for correction. If the statement was not dated, had the wrong room or computer identified, or was signed by the wrong person, the ISSO must return it to the DAA for correction. The ISSO is not authorized to make any "pen and ink" changes to the statement.

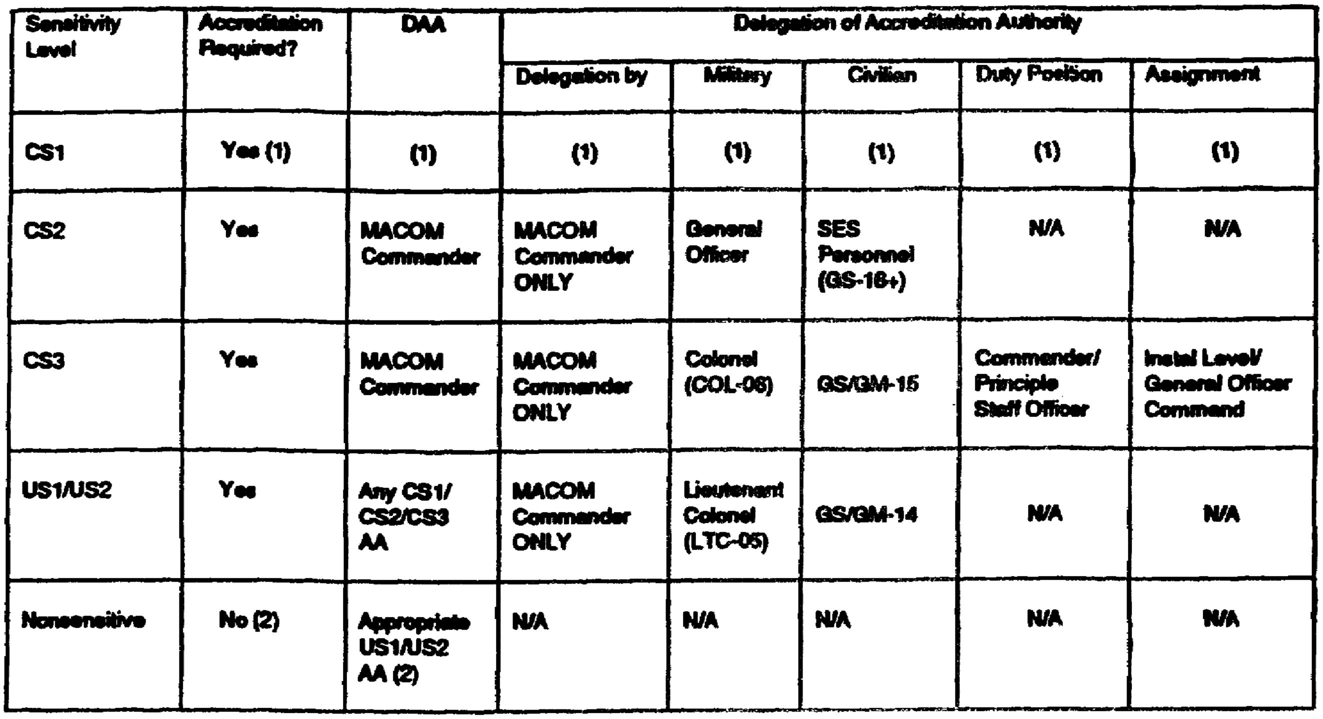
Reaccreditation is required in case of a change which will affect security or after three years. So, if the unit has its computers in an unauthorized location, they must be reaccredited for the new location. Until that is done, they must either move the computes back he authorized location or stop processing. Reaccreditation is also the "fix" for an unauthorized computer, for an unauthorized level of processing, or if the statement is more than three years old.

If a unit had an accreditation statement which was issued by anybody other than the DAA, the commander and the ISSO would have to request accreditation from the DAA. This would require them to resubmit the accreditation document/security plan to the DAA, long with he commanders request for accreditation.

If there is a problem and the commander and ISSO don't know how to "fix" that problem, they should contact the DAA for guidance.

An accreditation matrix is shown in Figure 3-4.

The following matrix indicates the sensitivity levels, whether or not accreditation is required, who the accreditation authority for each level is, and to whom accreditation authority may be delegated.



Sensitivity Level	Accreditation Required?	DAA	Delegation of Accreditation Authority				
			Delegation by	Military	Civilian	Duty Position	Assignment
CS1	Yes (1)	(1)	(1)	(1)	(1)	(1)	(1)
CS2	Yes	MACOM Commander	MACOM Commander ONLY	General Officer	SES Personnel (GS-16+)	N/A	N/A
CS3	Yes	MACOM Commander	MACOM Commander ONLY	Colonel (COL-06)	GS/GM-15	Commander/ Principle Staff Officer	Instal Level/ General Officer Command
US1/US2	Yes	Any CS1/ CS2/CS3 AA	MACOM Commander ONLY	Lieutenant Colonel (LTC-05)	GS/GM-14	N/A	N/A
Nonsensitive	No (2)	Appropriate US1/US2 AA (2)	N/A	N/A	N/A	N/A	N/A

Figure 3-4. Accreditation Matrix

(1) Special situation.

(2) No accreditation required, however designation must be approved, in writing, by an appropriate US1 or US2 accreditation authority.

LESSON 3

PRACTICE EXERCISE

The following material will test your grasp of the material covered in this lesson. There is only ONE correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. The security processing mode in which all users have the required security clearance, formal access approval, and a need-to-know for all information processed by the system is:
   ______________________________.

2. A computer is accredited at the CS2 level. By sensitivity level, identify the information it may be used to process.
   ______________________________.

3. A computer is accredited at the CS2 level. By classification, identify the information it may be used to process:
   ______________________________.

4. There are two occasions when the DAA will issue an accreditation statement. What are these two occasions?
   _________________________ and _____________________________.

5. What information cannot be processed on a new computer before it is accredited?
   ______________________________.

LESSON 3

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM	CORRECT ANSWER AND FEEDBACK
1.	Dedicated Security Mode (page 3-2).
2.	CS2, CS3, US1, US2, and Nonsensitive (page 3-4).
3.	TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (page 3-5).
4.	Initial Accreditation and Reaccreditation (pages 3-4 and 3-8).
5.	You can’t process any classified information, or any unclassified-sensitive information (page 3-3).

LESSON 4

PROTECTING COMPUTER STORAGE MEDIA

CRITICAL TASK: NONE

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn the various hazards to computer storage media and learn how to implement protective measures to overcome those hazards.

TERMINAL LEARNING OBJECTIVE:

ACTIONS: Define computer storage media, identify and define the hazards to storage media, and implement protective measures for computer storage media.

CONDITIONS: You will be given narrative information and extracts from AR 380-19.

STANDARDS: You will be able to recognize the hazards to computer storage media and develop effective countermeasures to overcome those hazards.

REFERENCES: The material contained in this lesson was derived from the following publication:

AR 380-19

Part A: Protecting Computer Storage Media

We must give particular attention to protecting computer storage media, because they are the primary means of storing computer programs and the information processed by computers, and they are the components of a computer which are perhaps the most vulnerable to loss and damage. This lesson will introduce you to computer storage media and procedures for protecting this storage media from harm.

Part B: Computer Storage Media Defined

First, what is "computer storage media?" "Media" is the plural of "medium" and includes "any substance or material on which information is represented or stored, and is used for input or output." There are two general categories of computer storage media:

Magnetic Storage Media: Floppy disks and hard disks are magnetic storage media; information is stored as tiny, invisible magnetic forces on the iron-oxide material which coats the surface of the disk.

Floppy disks: Most of you have used or have seen diskettes, also known as floppy disks." Floppies are about the most common means of storing programs and data, and virtually every PC has at least one floppy disk drive.

Hard disks: Hard disks are large capacity storage devices. A hard disk consists of several rigid magnetic disks permanently housed in a sealed unit. The disks are usually made of aluminum, coated with the same iron-oxide as the floppy disk. Many PCs also have a hard disk.

Optical/Magneto-Optical Storage Media: One of the newest things in computer technology is storing programs and information on compact discs (CDs). These CDs look like the CDs that play music, and are coming into widespread use. In this technology, computers use lasers to read and write information.

Part C: Hazards to Computer Storage Media

If storage media are vulnerable to loss and damage, what are the hazards? A “hazard” is anything that has the potential to damage or destroy a floppy disk, hard disk, or CD, and the programs or data stored on it. Computer storage media face several hazards:

Static electricity and magnetism: Static electricity, which you can get from simply walking across a carpet, and magnetic fields, which any telephone, radio or any electrical device generates, can have a devastating effect on storage media. Information which is stored magnetically can certainly be “unstored” magnetically. If you touch a floppy disk, the static discharge may alter the magnetically stored data, and you can lose your information. If you expose a floppy disk to a magnetic field, you will probably lose your information.

Contaminants: Ordinary contaminants like the tars and particles in cigarette smoke, doughnut crumbs, and coffee are probably the major reasons for disk failure. If you spill a cup of coffee on a floppy disk, its all over! If you then put that disk in your computers disk drive, you damage not only the floppy disk but your computer as well.

Temperature extremes: Temperature extremes, especially heat, are not good for magnetic storage media. The units which took computers to Saudi Arabia had some problems with the heat - temperatures there ranged from freezing at night to over 125 degrees in the daytime. If you leave a floppy disk in direct sunlight for any length of time, it will suffer damage.

User abuse: In Lesson 2 (The Threats to Army Computers), you found out that the authorized user is the leading threat, and that holds true for storage media as well. User abuse includes folding, bending, and dropping. Any rough treatment will likely damage your disk. Touch the recording surface and you leave an oily fingerprint. A sweaty fingerprint will probably rust or corrode the disks iron-oxide coating.

Part D: Damage to Computer Storage Media

Computer storage media all face the same hazards. However, the actual damage a hazard will cause depends on the type of storage media:

Floppy disks: Floppies are probably the most vulnerable of all the storage media, and any of the hazards will affect them.

Hard disks: Housed in a sealed unit, hard disks am relatively well protected from contaminants, but are still vulnerable to static electricity, magnetism, and temperature. And, the hard disk unit is very vulnerable to some types of user abuse; if you drop the unit on the floor, you are going to cause some major damage!

Compact discs (CDs): Of all the storage media, CDs are probably the most durable. They can take a lot of user abuse and are impervious to magnetism and static electricity. A fingerprint, dust, or coffee can usually be wiped off with no harm caused. But a CD can be scratched, and that will most likely mean lost information. Durability and large storage capacity are two masons that CDs are so popular.

Part E: Basic Protection for Storage Media

Give your computer storage media some basic protection and they, and your information, will last for a long time. The following are some basic measures for protecting storage media form common hazards:

Protect magnetic storage media from static electricity and magnetic fields.

Don't touch the recording surface. This goes for CDs, as well as for floppy disks.

Treat all storage media with care. For example, when you put a floppy in the disk drive, don't bend it.

A floppy disk comes in a protective envelope, and a CD comes in a plastic container. If the floppy or CD isn't in the drive, keep it in the protective envelope or container.

Protect all storage media from contaminants and don't eat, drink, or smoke when you are handling them.

Protect all storage media from temperature extremes and from direct sunlight.

Part F: Backup Procedures

"It's not "if" you'll lose your data, it's when!" The basic measures for protecting computer storage media will minimize, but cannot eliminate, the possibility that your media will be damaged and you will lose the information you spent time and effort on. Accidents happen! If you spill a cup of coffee on the floppy disk which contains your word processing program, that accident is as serious as the loss of your computer; in either case, you can't do your job.

You can’t eliminate accidents, but you can make provisions for recovering from them. Backup procedures, which include making copies of the storage media which contain your programs and important files, are a key element of computer security.

Users should make backup copies any time they process any information, but unfortunately it often takes the loss of an important file before users become “converts” to the routine of regular backup.

The commander and ISSO for each unit will establish procedures for regular and systematic backup, but as a "rule of thumb:”

1. As soon as you get a new program, back it up. An accident can damage a brand new program disk, so make the backup b you use the program even once. Make a backup, then try the program.

2. Each time you change or update a fib, back it up. if your disk is damaged after you have made extensive changes, you may forget what you changed and the updated information may be lost. At a minimum, it will take you considerable time and effort to reconstruct the changes.

3. If you store all of your programs and information on your computers hard disk, make sure that you have all of your programs and all of your information on backup floppy disks.

4. Keep in mind that an accident might damage all your disks, to include your backups. So, make yourself more than one set of backups and keep them in different locations.

Part G: Technologies of Computer Protection

The following gives a brief description of the main technologies of defense and some of their potential vulnerabilities. In describing vulnerabilities, this course does not mean to suggest that the technologies are riddled with holes or useless, only that they may not be foolproof. Particular attention is given to two recent technologies, location-based authentication and key escrow encryption.

Authentication. These technologies are used to determine the authenticity of users, network nodes, and documents. They are typically based on knowledge of secret information such as a password, PIN, or cryptographic key, possession of a device such as an access token or crypto card; and biometrics such as a thumb print or iris pattern. While all of these methods are valuable, they also have limitations Secret information may be vulnerable to guessing and cracking, hardware tokens to theft, and biometrics to false positives, false negatives, and replay. In addition, authentication controls are potentially vulnerable to subversion or by-pass.

Location-based authentication. International Series Research, inc. of Boulder, Colorado, has developed a new technology for authentication, called CyberLocatorTM, which uses space geodetic methods to authenticate the physical locations of users, network nodes, and documents. This is accomplished through a location signature sensor, which uses signals from the Global

signals from the Global Positioning system's worldwide satellite constellation to create a location signature that is unique to every location on Earth at every instant in time. This signature is used to verify and certify geodetic location to within a few meters or better. Because the GPS observations at any given site are unpredictable in advance (at the required accuracy level), constantly changing, and everywhere unique, it is virtually impossible to spoof the signature.

The CyberLocator technology is not vulnerable to many of the techniques in the attacker's toolkit, in part, because it does not rely on any secret information and it is not readily forged. In addition, it counters one of the attacker's most powerful tools, anonymity. Because the exact location of the intruder is revealed, it defeats looping and masquerading. It would be a strong deterrent to many potential intruders, who would be unwilling to make their locations known.

Location-based authentication would normally be used in combination with another method of authentication. its value added is a high level of assurance against intrusion from any unapproved location regardless of whether the other methods have been compromised. In critical environments, for example, military command and control, nuclear materials handling, telephone switching, air traffic control, and large financial transactions, this extra assurance could be extremely valuable. Location-based authentication also has applications besides access control, for example, implementation of an electronic notary function or enforcement of transborder data flows (e.g., export controls).

Cryptography. Various cryptographic techniques provide confidentiality protection (encryption) and authentication, which includes data integrity; user, host and message authentication; and digital signatures. They are used to protect both communications transmitted over open networks and data stored in computer files. Cryptographic systems can be implemented as stand-alone products or they can be Integrated into applications and network services, where they may be transparent to the user. They are potentially vulnerable to weaknesses in algorithms, protocols, key generation, and key management.

The encryption conflict. Encryption is essential for protecting classified national security information, unclassified but sensitive business and government information, and individual privacy. At the same time, in the hands of foreign adversaries, it interferes with signals intelligence. Terrorists, drug dealers, and computer intruders can use it to conceal their activities and stored records. Law enforcement agencies are concerned that as encryption proliferates worldwide, it could seriously imperil their ability to counter domestic and international organized crime and terrorism. It could cut off valuable sources of foreign intelligence. Even within an organization, encryption can cause problems. If keys are lost or damaged, valuable data may become inaccessible.

Access controls. These technologies are used to control access to networks, computers, applications, transactions, and information according to a security policy. Policies can be based on individual users, groups, or roles and on time of day or location. Access controls rely on authentication mechanisms to confirm the identity of users attempting access. They are typically integrated into both applications and systems software. Access controls are potentially vulnerable to bypass, failure to correctly implement the security policy, and ill-defined policies.

Firewalls. A firewall is a trusted computer system that monitors all traffic into and out of a protected network. it is frequently placed between an origination's internal network and the Internet with the objective of keeping intruders out and proprietary or sensitive data in. The firewall examines each incoming or outgoing message to determine whether it should be allowed to pass. Decisions can be based on protocol, source of destination address or port number, and message contents. Firewalls are potentially vulnerable to subversion, to malicious code that enter the firewall in a seemingly legitimate message, and to Ni-defined or incomplete policies.

Audit. Audit logs record security relevant activity, for example, successful and unsuccessful logins, execution of system commands and applications, and access to files and database records. Auditing can be performed at both the system level and the application level. Audit mechanisms are potentially vulnerable to being disabled or bypassed; audit records to tampering or deletion.

Intrusion detection/monitoring. Intrusion detection systems actively monitor a system for Intrusions and unauthorized activity. They typically inspect audit records, either after the fact or in real-time. They can look for particular events or event sequences, or for behavior that is abnormal. They are normally run under the direction of a security officer who specifies the events of interest and evaluates the results. Monitoring is analogous to the use of guards to keep watch over the physical premises of a protected site, either through direct surveillance or through video cameras. It is potentially vulnerable to false positives and false negatives, to being disabled, and to incomplete or false knowledge about misuse scenarios.

Anti-viral tools. These include scanners, which look for specified patterns; disinfectants, which remove viruses; and integrity checkers, which check for modifications to files and code. Potential vulnerabilities include failure to detect unknown viruses or to adequately protect checksums.

Vulnerability assessment tools. These are the same tools described earlier under the attacker's toolkit. They are potentially vulnerable to failure to detect a weakness or to misuse.

LESSON 4

PRACTICE EXERCISE

The following material will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. What are the two general categories of computer storage media?
   ______________________and ________________________.

2. Of all the hazards to floppy disks, what is probably the <u>major</u> reason for disk failure?
   ____.

3. You get a new word processing program. What should you do <u>before</u> you use the program?
   ____.

LESSON 4

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM CORRECT ANSWER AND FEEDBACK

1. Magnetic (Disks) and optical/magneto-optical (CDs)(pages 4-1 and 4-2).

2. Ordinary contaminants (page 4-2).

3. Make a backup copy (page 4-4).

LESSON 5

SAFEGUARDING CLASSIFIED INFORMATION

CRITICAL TASKS: 301-348-1001
301-348-6001

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn to identify computer-based classified information and the special requirements for its storage, handling, and disposal.

TECHNICAL LEARNING OBJECTIVE:

ACTIONS: Identify computer-based classified information, implement procedures for marking classified storage media, implement procedures for disposing of computer-based classified information, property destroy classified storage media, and properly safeguard classified computer-based information.

CONDITIONS: You will be given narrative information and extracts from AR 380-5 and AR 380-19.

STANDARDS: You will be able to recognize classified computer-based information and develop an effective security program to ensure that such material is properly protected in accordance with AR 380-5 and AR 380-19.

REFERENCES: The material contained in this lesson was derived from the following publications:

AR 25-400-2
AR 380-5
AR 380-19
DOD 5200.22-M
FM 19-30

Part A: Safeguarding Classified Information

We have discussed procedures for protecting computer storage media from loss and damage. Now we will discuss procedures for safeguarding classified information processed by computers. Anybody who has a security clearance should be fully aware of the procedures for safeguarding classified information. It should be pretty obvious that classified information stored on a floppy disk is going to require the same protection. However, a common problem in computer security is that many computer users have the mistaken idea that computer-based classified information is somehow not as classified as paper-based classified information.

Part B: Basic Safeguards for Classified Information

AR 380-5 requires that you receive an initial security briefing before you are granted access to classified information. The purpose of this briefing is to make sure that you understand the procedures for safeguarding classified information. When you were introduced to classified information it was probably in the form of a classified document, and AR 380-5 certainly is concerned with safeguarding classified documents. However, AR 380-5 applies to all classified information, regardless of its physical form or characteristics. Classified is classified, and computer-based and paper-based classified information will be given the same degree of protection. What's required for a classified document is also required for a classified floppy disk.

Both a classified document and a classified floppy disk must be:

Under the personal control or observation of an authorized person.

Guarded or stored in a locked security container (like a General Services Administration (GSA) approved security container) in accordance with paragraph 5-102, AR 380-5.

Accessed only by persons who have the appropriate security clearance and a need-to-know.

Marked with the overall (highest) classification and applicable associated markings in accordance with Chapter IV, AR 380-5.

Part C: Computer-Based Classified Information

One possible reason for that "perception" problem might be that users haven't been trained, and don't realize, what computer-based classified information looks like. When a computer is used to process classified information, there are several forms in which classified information might be found. The four items listed are collectively referred to as "computer media.

Storage media: If classified information is stored on a floppy disk, hard disk or compact disc (CD), it is classified material.

Work screen: If classified information is being processed and is displayed on the computer's screen, the screen is classified material.

Hard copy output: When any classified information is printed, the printout is classified material.

Memory: While classified information is being processed, the computer's internal memory contains classified material. Random access memory (RAM) is usually in the form of computer microchips.

Part D: Marking Classified Storage Media

Classified storage media must be safeguarded as classified material and must be marked in accordance with Chapter 4, AR 380-5. Computer storage media are a special category of classified material as far as marking.

Basic Identification: As well as security markings, computer storage media require other external labels. You can't tell what information is stored on a floppy disk by looking at it. Therefore, it is recommended that all computer storage media have some form of basic external identification, such as a label identifying, at a minimum, the disks contents and date. This procedure is not required by AR 380-19, but it is recommended that storage media be identified with this basic information. The best procedure is to use a label formatted in accordance with AR 25-400-2, The Modem Army Recordkeepkig system (MARKS), similar to the following example:

> ABCD-EF (525n) Disk
> #415
>
> XX Corps OPLAN 98-7
> MSG Swendsen 6 Jul
> 98

Organization and MARKS file number: The organization or unit which created or owns the medium. The units designation or the units office symbol may be used (ABCD-EF).

Permanent ID number: A unique identification number or serial number assigned by the unit (Disk #415).

ID title or name: A title which identifies the contents of the medium. This is alike a document title (XX Corps OPLAN 98-7).

User The primary user is probably the individual who created the medium, and can be identified by name or position (MSG Swendsen).

Date created: The date the medium was created (6 Jul 98).

Part E: Overall Classification

Computer storage media on which classified information is stored must be marked with the overall (highest) classification.

Both paragraphs 2-20a. AR 380-19, and 4-304a, AR 380-5, require that the following specific Standard Forms (SF) be used to indicate the overall classification on computer media, and allow for no exceptions:

SF 706 (Orange Top Secret Label).
SF 707 (Red Secret Label).
SF 708 (Blue Confidential Label).
SF 710 (Green Unclassified Label).

These colors are the same as the colors of the classified document cover sheets.

In addition to the use of these labels, any and all warning notices or handling caveats that may apply to the data stored on the specific media, such as WNINTEL, must also appear. In these cases, plain white address labels with the applicable caveats stamped on them will suffice.

Making Floppy Disks

As a general rule, if a unit processes only US1, US2, or Nonsensitive material, diskettes and other media do not need to be marked as Unclassified. If the unit does have CS1, CS2, or CS3 accredited systems, however, all media must be marked to indicate classification. Neither AR 380-5 nor AR 380-19 Indicate exactly how computer media is to be marked, as long as you use the required standard forms to indicate classification, and have all the other required information (caveats, classification authority, downgrading/declassification instructions, etc.) on the disks.

Of course, if your MACOM supplement to AR 380-19, your unit commander, or your unit ISSO have established a particular way of marking disks, you must comply with it.

Paragraph 4-300, AR 380-5, calls for "conspicuous" markings on special categories of classified material, so the appropriate classification label should also be placed on the front and back of the protective envelope. Storage containers, other than your security container, should also be labeled.

Disks of Different Colors

Another method for identifying floppy disks on which classified information is stored is the use of uniquely colored diskettes, using the same color scheme as that used for the classification labels; orange for TOP SECRET, red for SECRET, and so on.

These colored disks are available from a number of commercial sources. Also, they are supposed to be coming into the Army supply system.

One advantage of colored disks is visibility; It would be easier to spot a red disk containing classified information if it was left on a desk by mistake.

Another advantage is security, if a unit used blue disks for CONFIDENTIAL and red disks for SECRET, it might prevent somebody from copying a SECRET file onto the wrong disk by mistake.

Marking Hard Disks

A removable hard disk unit on which classified information is stored will be labeled with the basic identification, classification, any additional warning notices, the classification authority, and the downgrading or declassification instructions.

The unit is usually rectangular, and the classification labels will be placed in conspicuous locations on the hard disk; top, bottom, and all four sides.

Most hard disk units come in a cushioned carrying case which helps protect them from shock You must also mark this case with all the required labels.

Marking Compact Discs (CDs)

Labeling a CD is a problem; an SF 707 is required for a CD on which SECRET information is stored, but there is not enough room on the back (data side) of a CD for the SF 707 or the other labels.

A recommended solution is to place all of the required labels (SF 707, basic ID, classification authority line, and the declassification or downgrading instructions) on the front (label side) of the CD and on the protective container. Then label the back of the CD itself with the classification, using a label small enough to fit on the CDs hub. This way the CD is still labeled “SECRET” on both sides.

Part F: Disposing of Computer-Based Classified Information

When a classified document is no longer needed for current operations, you get rid of it. Disposing of a paper-based classified document is pretty easy; you remove it from the files and destroy it immediately or throw it in a bum bag. Disposing of computer-based classified documents which are stored on some type of magnetic or optical storage media is not always so easy.

Part G: Explanation of terms

Before we discuss disposing of computer-based classified information, there are four terms which you must understand:

Declassification: As used in AR 380-19, this term has a different meaning than the one you learned from AR 380-5. As used in AR 380-19, declassification” is an administrative procedure to determine that classified information stored on a computer storage medium has been removed or overwritten sufficiently to permit reuse in an unclassified environment .

Purging: A procedure used to totally and unequivocally erase or overwrite all information stored on computer storage media. Purging is one prerequisite to declassification of magnetic media.

Degaussing : A procedure used to erase all information stored on magnetic media by exposing it to a magnetic field generated by a device called a “degausser."

Overwriting: A procedure used to erase all information stored on computer storage media by using a computer program which repeatedly (at least three times) overwrites all locations with ones and zeroes, or random characters.

Part H: "DELETE," "ERASE," and "FORMAT"

Before we discuss how to dispose of classified information, lets take a look at some things which DON'T work. If you store classified information on a floppy disk or hard disk, there are some computer commands which seem to erase classified information from the disk, but, in reality, DO NOT purge information from the media, and DO NOT meet the prerequisites for declassification.

"DEL" (delete) and "ERASE" are MS-DOS (a program which controls the basic operation of a PC) commands which delete a file from a disk. Word processing programs also have a delete or erase command. These commands DO NOT actually erase the information! They only remove the file name from the disk file directory, which is a kind of table of contents for the disk.

"FORMAT" is an MS-DOS command which prepares a disk to receive files. If you format a disk on which files are stored, only the disk file directory and volume table of contents (VTOC) are blanked out The directory and VTOC are removed, but he files and all the information have NOT actually been erased.

Part I: "RESTORE"

There are a number of commercially available computer utility programs which can "unerase" deleted files and can recover files from a formatted disk. Using such software, any deleted or erased file can be recovered. If you store a SECRET file on a disk and delete or erase that SECRET file or format that disk, that disk is still SECRET.

Part J: Approved Methods for Purging Computer Media

If "erase" or delete" doesn't purge your computer media, what does? Paragraph 2-21, AR 380-19, describes the methods for purging which are the ONLY ones approved for use in the U.S. Army. These methods DO purge all information and DO not meet the prerequisites for declassification.

Volatile Random Access Memory (RAM): Volatile RAM (internal memory chips which do not retain their data when electrical power is removed) can be purged by overwriting all locations with any character, or by performing a power off/on cycle (turn the power off, then on, and then off again).

Floppy disks (magnetic): Floppy disks (both 5.25 Inch and 3.5 inch) can be purged by degaussing with a Type I or Type I degausser. These degaussers are listed in NSA (National Security Agency) publication, "Information Systems Security Products and Services Catalogue." There are a lot of degaussers on the market, but you can ONLY use those that are approved by the NSA.

Hard disks (magnetic): Hard disks can be purged by degaussing with a Type I or Type II degausser. They can also be purged by overwriting all locations as described in Table 2-2, AR 380-19.

Magneto-optical discs: CDs CANNOT be purged. If classified information is stored on a CD, it is permanently classified!

Part K. Declassifying Computer Media

Declassification, as used in AR 380-19, is an administrative procedure. Before a floppy disk on which classified information has been stored can be treated as unclassified material, it must be purged. Then, the ISSO must verify that the method of purging meets the requirements of Tables 2-1 and 2-2, AR 380-19, and that all classified information has been TOTALLY purged. Them are risks involved with purging and declassifying computer media:

Time and temperature: If classified information has been stored on magnetic media for an extended period of time, or if the magnetic media is stored in high temperature conditions (120 degrees Fahrenheit or greater), it is more difficult to erase the information completely.

Equipment software, or human error: An approved degausser may not work. The ISSO may not follow the directions on using the degausser. A computer program may not overwrite all locations on a hard disk.

Damaged media: If you store classified information on a hard disk and then drop it on the floor, you have a problem! If the hard disk is damaged, it will probably not be possible to purge it.

NOTE: Given their low cost and the risks involved, destruction of floppy disks is more appropriate than declassifying.

Part L: Nonremovable Storage Media

Paragraph 2-22a, AR 380-19, says "Using a computer with nonremovable, nonvolatile media for processing classified information is discouraged."

Explanation of terms: These two terms, "nonremovable" and “nonvolatile,” may be new to you, so let us take a look at what they mean.

Removable media: Floppy disks, CDs and certain models of hard disks are designed to be easily and routinely removed by the user.

Nonremovable media: Hard disks, computer chips, and other components which can store information, and are not designed to be easily and routinely removed by the user. They can be removed only by taking the computer apart These are also called “fixed” media Unless we take the PC apart a “fixed” hard drive stays where it is.

Volatile computer media: Computer media which lose the information stored in them when electric power is removed. Most PCs use volatile RAM (random access memory) to store the information which is being processed. That’s why you lose all the information you are working on when you have a power failure.

Nonvolatile computer media: Computer media which does not lose the information stored in it when electric power is removed. Floppy disks, hard disks, and CDs are nonvolatile. If you store information on a floppy disk, remove it from your PC, and turn off the power, that information is still on the floppy. Laptop computers usually have a backup battery in them which retains data in the memory chips even when they are not in use. Computers which operate from battery power are, therefore, nonvolatile.

The reasons for discouraging the processing of classified information on a computer which has a “fixed" hard disk or battery-powered memory chips are that if classified information is processed, it must be assumed that classified information has been stored on the hard disk or is still in the memory chips. The computer user might not intentionally store classified information on the hard disk, but through human or computer error, classified information can be stored on the hard disk without the user being aware of it. Some word processor programs automatically store data on the hard disk periodically. And, given the problems with purging and declassification, if classified information is stored on a fixed hard disk, it may not be possible to purge it

If classified information is stored on a “fixed" hard disk, the hard disk unit and the computer must be marked, safeguarded, and stored as classified material.

Part M: Destruction of Storage Media

When no longer needed or damaged, computer storage media should be destroyed. The approved methods for destroying classified material, to include computer storage media, are found in Appendix K, AR 380-5. And, as we know from paragraph 9-101 of AR 380-5, burning is the preferred method of destroying classified information. Here is a summary of the approved methods for destroying storage media:

Floppy disks

The preferred method of destruction is burning. The flexible magnetic disk should be removed from the protective envelope and burned following the procedures in paragraph K-4b(1), AR 380-5. If not burned, the disk should be cut or shredded following the procedures in paragraph K-5d, AR 380-5. This paragraph describes shredders. Something that must now be kept in mind when burning diskettes, however, is a provision in AR 380-5 which states that any device used to bum plastic-based waste must comply with the provisions of the Environmental Protection Agency (EPA) Federal Clean Air Act. As of this writing, the only device approved by the EPA is a pyrolytic furnace.

Hard disks: The aluminum disks should be removed from the hard disk unit and destroyed following the procedures in paragraph K-5e, AR 380-5. This paragraph describes procedures for destroying equipment and devices; burning, melting, sledge hammer and hacksaw demolition, and crushing. If you ever have to destroy a hard disk by melting, your best bet is to go to the engineer yard and find yourself an acetylene torch. If an engineer employee is going to perform the destruction, they must have an appropriate security clearance.

Compact discs: The procedures described in paragraph K-5e of AR 380-5 for destroying equipment and devices, such as hard disks, can be used to destroy a compact disk as well.

Part N: Other Classified Material

When a computer is used to process classified information, there are forms of classified information besides storage media which must be protected. Besides the floppy disks, you must also protect all the rest of this classified material.

The work screen and the computer. When classified information is being processed, you must make sure that any classified information which is displayed on the work screen cannot be seen by unauthorized persons. And, when classified information is being processed, the computer and its associated peripherals must be safeguarded as classified material, since classified information will also be stored in internal memory. "Associated peripherals" means the monitor, the printer, and any other computer equipment connected to the computer.

If possible, all classified processing should be done in a locked room which has no windows. This is not always possible, and the computer you are using to process classified information may be located in an "open" office. In the open office, the use of temporary partitions or curtains, or the removal of unauthorized persons might be required. If the office cannot be locked, guards and "no entry" signs will help to prevent unauthorized access.

Hard copy output: Paragraph 4-305, AR 380-5, describes the requirements and procedures for marking classified documents produced by computer systems. Classified printouts can be marked automatically by the system, if it has this feature, or marked manually, like marking a typed document

Miscellaneous material: A printer ribbon used to print classified information requires the same protection as a typewriter ribbon used to type classified information.

Part O: Recommended Procedures for Processing Classified Information

Your commander, ISSO, and TASO will develop procedures for safeguarding computers which process classified information in your unit. These are recommended procedures which should be followed when using a computer to process classified information.

Make sure that the computer is accredited for the level of classified information to be processed.

Physically disconnect any connection to another computer, unless the other computer is required for the processing, and classified information is transmitted between the two by "secure means". Chapter 4, AR 380-19, describes secure means for transmitting classified information.

Physically disconnect any peripherals, such as disk drives or printers, which are not required for the classified processing.

Secure the areas where the classified processing will be done to make sure that an unauthorized person cannot get access to the computer, or see classified information displayed on the work screen.

Make sure that all persons who will have access to the computer, or who will be able to see the work screen have an appropriate security clearance and a need-to-know for all classified information to be processed.

Make sure that all classified information is stored only as approved by the ISSO. Given the problems Involved with declassifying computer storage media, it is recommended that only removable floppy disks be used for storing classified information.

Mark all storage media and hard copy output in accordance with Chapter 4, AR 380-5, and the ISSO's instruction.

When you are done processing, secure all classified material, such as removable storage media and printouts.

Power down the computer to purge all classified information from internal memory. Remember, the ISSO must verify this.

LESSON 5

PRACTICE EXERCISE

The following material will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. You have stored a SECRET document on a floppy disk. How must you store that disk?
   ________________________________.

2. Using uniquely colored floppy disks, what color should you use for a disk on which CONFIDENTIAL information is stored?
   ________________________________.

3. What is a Standard Form (SF) 710, and what is it used for?
   ________________________________.

4. As used in AR 380-19, what does the term “removable AIS media” mean?
   ________________________________.

5. What is the preferred method for destroying a floppy disk on which classified information has been stored?
   ________________________________.

6. Where would you look to find the approved methods of destruction for a hard disk on which classified information has been stored?
   ________________________________.

LESSON 5

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM CORRECT ANSWER AND FEEDBACK

1. In a locked security container IAW paragraph 5-102, AR 380-5 (page 5-2).

2. Blue (page 5-5).

3. It's a (green) label for marking unclassified computer media (page 5-4).

4. It is designed to be easily and routinely removed by the user (page 5-8).

5. Burning (page 5-9).

6. AR 380-5. (Appendix K, paragraph K-5e)(page 5-9).

LESSON 6

MISCELLANEOUS COMPUTER SECURITY REQUIREMENTS

CRITICAL TASK: 301-348-6001

OVERVIEW

LESSON DESCRIPTION:

In this lesson you will learn computer security training requirements, PC security measures, the requirements that must be met before using an employee-owned computer in an Army office, measures designed to prevent software piracy, and protection against malicious software.

TERMINAL LEARNING OBJECTIVE:

ACTIONS: Identify who is responsible for computer security training within each unit, recognize the extra security measures that are required for personal computers (PCs), advise personnel of the restrictions against the use of privately-owned computers, guard against the illegal copying of government-owned software, and recognize the problems associated with malicious software.

CONDITIONS: You will be given narrative information and extracts from AR 25-1, AR 380-5 and AR 380-19.

STANDARDS: You will be able to advise unit commanders, security managers, and ISSOs/TASOs on computer security training requirements outlined in AR 380-19, and provide advice and assistance to units concerning the unique security problems associated with small computers, the use of employee-owned computers, software piracy; and malicious software (viruses).

REFERENCES: The material contained in this lesson was derived from the following publications:

AR 25-1
AR 380-5
AR 380-19
DOD 5200.22-M
FM 19-30

Part A: Security Training and Awareness

"There is an explosive situation brewing. On the one hand, the press, television, and movies make heroes of vandals (hackers) by calling them whiz kids. On the other hand, the acts performed by these kids will soon be punishable by years in prison.

I have watched kids testifying before Congress. It is clear that they are completely unaware of the seriousness of their acts. There is obviously a culture gap. The act of breaking into a computer system has to have the same social stigma as breaking into a neighbors house. It should not matter that the neighbor's door is unlocked. The press must learn that the misguided use of a computer is not more amazing than drunk driving of an automobile.

Ken Thompson
AT&T Bell Laboratories

Part B: Who is Responsible?

The most comprehensive security procedures, the best written security standing operating procedure (SOP), and the most sophisticated security hardware and software in the world will amount to nothing, if computer users are not security conscious.

The National Computer Security Council reports that the number one computer problem is a "lack of awareness and concern among computer users, which leads to problems of neglect… in general, not knowing or caring about good computer security practices."

This lack of awareness on the part of users is the cause of most problems. If a user does something wrong, it is usually ignorance of security procedures and not a willful disregard.

The individual computer user is the most important person in maintaining the security of computer systems. If this security is to be maintained and effective, each user must develop a "security mind-set." The properly trained and motivated user is the ultimate countermeasure to the threats facing Army computers.

If security is to work, it must be accepted by the people who must live with it and enforce it on a day-to-day basis. Users must be educated so that they understand why security is necessary, what security measures are used and how they work, and who is responsible for what.

Part C: Required Security Training

AR 380-19 requires that all personnel who manage, design, develop, maintain, or operate a computer receive security and awareness training consisting of an initial briefing and periodic training.

Part D: Initial Security Training

The first security training which computer users receive is the initial briefing. This briefing should be given upon arrival at the unit, and should be given before the person begins his assigned duties. A user should not be allowed to use a computer to process any classified or unclassified-sensitive information until he has been given this briefing. The initial briefing should be tailored to the computer which the user will be operating and to the units security measures. The purpose of the initial briefing is to make sure that the computer user understands:

Why security? A computer can be "user friendly," or a computer can be secure, but it cannot be both. To the user, security means that it is going to be harder to get his work done. An essential ingredient of the training program is threat awareness; users must be made aware of the threats involved with processing classified information. Through training, users will understand why security is required and accept it.

Who is responsible for what? Everybody is responsible for security, but each person in the unit has specific responsibilities. The computer user must be informed of the commanders responsibility for, and interest in, security. The user must be informed that the commander has appointed an ISSO and TASOs as security experts, should be told who they are, and how to contact one of them. The user must understand that he is responsible for complying with the units security measures, and contacting the ISSO or TASO if he has a problem or question regarding computer security.

Part E: Periodic Security Training

Computer users must also be given periodic refresher training, preferably on an annual basis like the other security training required by AR 380-5. The purpose of periodic training is to remind personnel of security policies and procedures, remind personnel of their security responsibilities, and make sure they are aware of any new policies and procedures. Periodic training can consist of formal instruction, security bulletins, security posters, films or video tapes, or a combination of these training methods.

Part F: PC Security Measures

Most of the Army’s 400,000 or so computers are small computers, also known as PCs. The security of these PCs and other “office automation systems," like word processors, is on of the biggest problems facing the Army today. Practically every unit in the Army uses PCs for typing, information filing and retrieval, sending and receiving electronic mail, and other information processing tasks.

Although PCs perform essentially the same functions as large computer systems, PCs have some characteristics which present special security problems. In general, the differences between large computer systems and PCs (and the source of those special problems) are physical access, built-in security features, and the nature of the information processed.

Traditionally, large computer systems were found only in a centralized data processing department. They were located in a central computer room, and were provided with considerable physical and environmental protection. Built-in security features, such as password systems, protected information from unauthorized access. The information itself was often in the form of large volumes of unprocessed "raw data.”

Today’s electronic office presents unique security problems as computing has moved out of the computer room and into the work area. The typical office is an open environment, and the office PCs are scattered throughout the work area on tables and desks. Most PCs do not support, or are not equipped with, built-in security features which isolate computer users from classified or sensitive information. Finally, the information processed by and stored on PCs is often in the form of “finished” documents which can be more sensitive than the raw data stored in the large computer system.

PCs are, by their very nature, extremely difficult to secure. The PC and the information it processes are highly vulnerable to unauthorized access and theft. Despite this fact, the Army is using PCs on an ever-increasing basis to process and store classified and sensitive information. When a PC sits out in the open, protecting it and the classified and sensitive data stored on it is a challenge.

Part G: Physical Protection

Since most PCs are located in an open office environment and lack built-in security features, physical security measures are the primary line of defense. The first problem is to protect the PC and the sensitive data processed and stored on it from unauthorized access. Unauthorized access is any intrusion by a thief, a foreign country agent, or a dishonest employee who wants to obtain information; destroy or alter information; steal, damage, or destroy the PC; or use a PC.

Every office has some physical security procedures in use, and these procedures apply to the PC as well. Generally, every office is locked at the end of the day and when nobody is in the office. Somebody usually does an end-of-day security check. Classified and sensitive information is secured when not in use, and we can expect employees to challenge a stranger who enters the office.

However, there are limits to what locked doors and windows can do to stop a determined thief, and some additional physical security measures should be considered. PCs are small and light enough for a single person to carry off, and are easily marketable items for the thief. A few simple physical security measures can stymie a thief.

Bolting down the PC: Physical security for the PC begins with fastening the PC, and its peripherals, to a table or desk. There are a number of commercially available locking systems. Most rely on wire cable and locks similar to those used to secure a bicycle. Another approach involves encasing the PC in a lockable cabinet or workstation. This won’t protect your PC from a well-prepared thief armed with the right tools, but it might send him looking for easier pickings.

Marking the PC: The most cost-effective anti-theft measures are undoubtedly marking each piece of computer equipment with the unit’s name. You can mark the equipment with indelible markers, stencils and paint, or an engraving tool. The thief will have a hard time fencing a PC that is engraved with “Property of the United States Army.”

Locking up the keyboard: Most PC keyboards are removable, and a good measure against unauthorized use is removing the keyboard and locking it up when the PC is not being used. This won’t stop a thief from stealing the PC, since replacement keyboards are relatively cheap, but at least you can control its use.

Part H: Environmental Protection

PCs are designed to be used in the typical office environment, an unlike large computer systems, do not require air conditioning. Generally, if you are comfortable, so is your PC. However, all computer systems, regardless of size, have four primary environmental enemies:

Dust and other contaminants: Good housekeeping is a must! The PC and the surrounding area must be kept clean and free of dust The PC and the surroundings should be vacuumed, rather than dusted. A dry cloth is only going to kick up more dust, generate static electricity, and add to the problem. As a measure to protect the PC from carelessness and accidents, users should be prohibited from eating, drinking, and smoking while using the PC, and within six feet of the PC. The tars and smoke particles from cigarette smoking are virtually guaranteed to gum up the PC, so unless the ventilation is good, don’t even smoke in a room which contains a PC.

Fire: Good housekeeping and a no smoking policy will reduce the threat of fire. In case of fire, there must be a fire extinguisher within 50 feet of each piece of computer equipment. A computer is an electrical device, and water-type fire extinguishers must not be used in the vicinity of the PC. Water will damage the PC. Also, water will conduct electricity from the PC to the fire extinguisher, and you may be electrocuted.

Static electricity: Static electricity, which you can generate by simply walking across the carpet, can damage not only a floppy disk, but the microchips Inside the PC as well. Static can be handled in a couple of ways. By training, users can get into the habit of touching a grounded object (other than the PC) to discharge the static. Posting a sign near each PC will remind users to do this before touching the PC. Commercially available anti-static carpet, pads, and spray are another option, but cost money and are not really that effective. A cheap and fairly effective solution to the problem of carpets and static is mixing fabric softener with water and spraying the carpet around the PC.

Electrical power: Computer power protection is like insurance; the more you want, the more you have to pay. If the local power supply is very poor, an uninterruptable power supply (UPS) might be necessary. A UPS will backup the power in case of a power failure, but will cost at least several hundred dollars. For $25-$50 you can get a surge/electromotive interference/radio frequency interference (EMI/RFI) power strip which won’t provide backup owner, but will protect your PC for a power surge. And, for no cost but temporary down time, you can turn off the PC and unplug it in case of an approaching electrical storm. You should get into the habit of routinely unplugging your computer at the end of the day, and turning it off when it will not be used for a period of time.

Part I: Employee Owned Computers

An “employee-owned computer” is a privately owned computer which belongs to a soldier or a civilian employee; it is not owned by or leased by the U.S. Army or the U.S. Government.

Although employee-owned PCs are authorized for use in the government work place, it is strongly discouraged. It is discouraged because an employee may become dependent on his other PC and may accidentally process information that is not authorized for his or her PC (paragraph 5-4b, AR 5-1). Before the Army established this policy on the use of employee-owned computers at the work site (office), it was common practice for soldiers and civilian employees to bring their PCs into the office and use them to process Army related (official) work. This caused problems, and that is why the use of employee owned computers is now discouraged:

Dependence: The employee owned PC may become so "mission-essential" that the unit cannot perform its mission without that PC.

Liability: If the employee owned PC is stolen or damaged at the work site, the owner can file a claim for reimbursement with the Claims Office.

Software piracy. The use of employee owned PCs at the work site encourages the unauthorized copying and use of Army software.

Security: Since the employee owned PC is not Government property, the owner and other users tend to disregard security procedures.

The use of employee owned computers at the work site is discouraged, but not prohibited. Commanders may approve or disapprove their use, and will establish appropriate procedures for their approval and use in the unit. The commander must approve the use of employee owned PCs both at and off the work site. If approved for use, certain restrictions apply to the use of employee owned PCs (or any other employee owned computers):

The employee owned PC must comply with all provisions of AR 380-19, to include accreditation.

Government related work processed by the employee owned PC is the property of the Untied States Government

Classified information will not be processed on an employee owned PC. Only UNCLASSIFIED information may be processed.

Part J: Software Piracy

"In 1988, $3.5 billion in microcomputer software was sold worldwide. During that same time, another $3 billion in sales was lost to free distribution - better known as software piracy."

J.B. Musgrave
Rainbow Technologies

Software piracy: To reproduce computer programs without authorization, especially in infringement of copyright.

One of the problems facing software publishers is the wholesale pirating of the computer programs they produce and market. Ken Wasch, Executive Director of the Software Publishers Association (SPA), says that for every legitimate copy of PC software in use, an additional copy exists. The Copyright Act of 1986 covers computer programs, and makes the pirating of software Illegal. You do not have the right to make and distribute extra copies of a computer program to your friends any more than you have the right to copy and distribute "The Hunt for Red October."

The SPA has begun to fight back against software piracy through the establishment of a toll-free, confidential piracy hot line, 1-800-PIRATE. Early results from this effort indicate that the majority of calls are from co-workers of software pirates, and the average courtroom sentence has been a $10,000 fine against pirates for violation of the Federal Copyright Act.

Most of the computer programs used on Army-owned PCs are commercially available programs which are licensed from software publishers. The Army does not own these programs, but has only paid for the right to use them. These programs are covered by the Copyright Act of 1976, and by some sort of license agreement between the Army and the software developer. The copying of such programs is either prohibited or limited by this agreement The following is an example of a software license agreement

SOFTWARE END-USER LICENSE AGREEMENT

IMPORTANT: This software is a proprietary product and is protected by copyright laws. It is licensed (not sold) for use on a single machine, and is licensed only on the conditions that you agree to the terms of this AGREEMENT.

1. USE. You may use the software on a single machine. The software may be removed form one machine and physically transferred to another machine, but shall not under any circumstances be used concurrently on more than one machine.

2. COPY. You may copy the software into any machine-readable or printed form for backup purposes in support of your use of the software on a single machine.

3. TRANSFER. You may transfer the software together with this license to another party, but only if the other party agrees to accept the terms and conditions of this AGREEMENT. If you transfer the software and license, you must at the same time either transfer all copies, whether in printed or machine-readable form, to the same party or destroy any copies not transferred.

EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, ANY USE OF COPYING OF THE SOFTWARE, INCLUDING DOCUMENTATION, OR TRANSFER OF THE SOFTWARE IS PROHIBITED.

Under the terms of the above agreement, your right to use and copy the computer program is limited to the following:

If your PC has a hard disk, you are authorized to copy to computer program from the original disk to the hard disk for day-to-day use. Once you copy it, you must not use the program on a second PC. After you copy it, secure the original disk. If you want to use the program on a second PC, you must first erase the program from the hard disk in the first PC. The program may not be used on two PCs at the same time.

If your PC has only floppy disk drives, you are authorized to make a backup copy of the original program disk for day-to-day use. If you have several PCs In the office, you may use the copy on any of those PCs. However, you may not make two copies and use the program on two PCs at the same time. After you make your backup copy, secure the original disk.

If you transfer (give) the program to another party (a person, office, or unit), they must also comply with the software license agreement. You must give that party all copies of the program and all documentation. Any copies you do not transfer must be destroyed. If you copied the program onto your PCs hard disk, you must erase it.

NOTE The above software license agreement is an example of a typical license agreement, and does not apply to all Army-provided software. Each Army-provided computer program will be covered by a unique agreement, so before you copy any program, read the agreement. If you cannot understand the agreement, check with your ISSO. Software piracy is a violation of the Copyright Act, the license agreement, and Army policy ... “proprietary software will not be copied or duplicated unless permitted by the terms of the contract. (paragraph 5-3e, AR 25-1).

Part K: Malicious Software

In the last couple of years, stores about computer viruses have ripped through the computer community like a prairie fire. Reports of data-killing and program-killing viruses have made for some sensational reading, but a virus is only one type of destructive computer program.

Part L: Destructive Programs

Virus: A virus is a program which, unknown to the user, performs a destructive act and can reproduce Itself. If you use an infected floppy disk on your PC, the virus will copy itself to the hard disk. Once the hard disk is infected, any floppy you use on the PC gets infected as the virus replicates Itself from the hard disk to the floppy. If you use that inflected floppy on a second PC, the virus spreads to it. A virus can be a logic bomb or a Trojan home.

Logic bomb: Also known as a “time bomb," this is a computer program which performs a destructive act, like erasing computer programs or data, when triggered by a particular date or event. The “Columbus Day” virus is the one which has received the most publicity.

Trojan horse: This type of computer program is named after the Trojan Horse in Greek mythology which looked harmless, but held destruction within. A Trojan Horse contains code which appears to perform a legitimate act, such as maximizing a hard drive's efficiency, but actually performs a destructive act. The "Jerusalem" virus was of this genre.

Part M: Infection Protection

"Aristotle said that the unexamined life is not worth living. We say the unexamined program is not worth running."

PC Magazine

PCs are especially vulnerable to "software attack" because of the large amount of software exchanged by users. There is no foolproof way of preventing an attack or detecting a destructive program which gets into your software, but to help keep your software "infection free," you should:

Use only Army-provided software on your PC. Any software could contain one of these destructive programs, but most Army-developed software and Army-provided commercial software is safe. If you receive an original disk in a "shrink-wrap" package, it is probably not infected.

Use "public domain" software with caution! This software usually comes from computer clubs or computer bulletin boards. Public domain software is not covered by copyright, and anyone can copy it and use it, without restriction. This software is a leading source of infection, and unless it comes from a known and trusted source, don't use it.

Don't use pirated software! Pirating software is illegal, and pirated software is a major breeding ground for destructive programs.

Make frequent backup copies of your data disks. This will not prevent a software attack, but it will help you recover from one.

Don't let a stranger use your PC. Make sure that only authorized persons use your PC, and make sure that repair personnel perform only authorized repairs or modifications.

Finally, consider using one of the various "vaccine" program which are designed to detect viruses in your software.

LESSON 6

PRACTICE EXERCISE

The following material will test your grasp of the material covered in this lesson. There is only one correct answer for each item. When you have completed the exercise, check your answers with the answer key that follows. If you answer any item incorrectly, study again that part of the lesson which contains the portion involved.

1. The most important person in maintaining the security of computer system is:
   ____.

2. AR 380-19 requires that all personnel who manage, design, develop, maintain, or operate a computer system receive security and awareness training consisting of
   ____________________and ___________________.

3. The use of an employee-owned computer and software to process Government related work at the work site is:
   ____.

4. The three major types of destructive programs are:

   ____________________, _______________________,

   and_________________.

LESSON 6

PRACTICE EXERCISE

ANSWER KEY AND FEEDBACK

ITEM CORRECT ANSWER AND FEEDBACK

1. The individual computer user (page 6-2).

2. An initial briefing and periodic training (page 6-2).

3. Discouraged but not prohibited (page 6-6).

4. Logic bomb, Trojan horse, and Virus (page 6-9).